SmartSwitch 2200 Series

(2E253, 2H252, 2H253, and 2H258)

Standalone Switches

Local Management User’s Guide

9033650-04

ENTERASYS
NETWORKS™

NOTICE

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document and its web site without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this document is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810

Part Number: 9033650-04 June 2003

Version: Information in this guide refers to SmartSwitch 2200 Series firmware version 5.05.xx.

ENTERASYS NETWORKS, INC.
PROGRAM LICENSE AGREEMENT

**BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT,
CAREFULLY READ THIS LICENSE AGREEMENT.**

This document is an agreement ("Agreement") between the end user ("You") and Enterasys Networks, Inc. on behalf of itself and its Affiliates (as hereinafter defined) ("Enterasys") that sets forth Your rights and obligations with respect to the Enterasys software program (including any accompanying documentation, hardware or media) ("Program") in the package and prevails over any additional, conflicting or inconsistent terms and conditions appearing on any purchase order or other document submitted by You. "Affiliate" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. This Agreement constitutes the entire understanding between the parties, and supersedes all prior discussions, representations, understandings or agreements, whether oral or in writing, between the parties with respect to the subject matter of this Agreement. The Program may be contained in firmware, chips or other media.

BY INSTALLING OR OTHERWISE USING THE PROGRAM, YOU REPRESENT THAT YOU ARE AUTHORIZED TO ACCEPT THESE TERMS ON BEHALF OF THE END USER (IF THE END USER IS AN ENTITY ON WHOSE BEHALF YOU ARE AUTHORIZED TO ACT, "YOU" AND "YOUR" SHALL BE DEEMED TO REFER TO SUCH ENTITY) AND THAT YOU AGREE THAT YOU ARE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES, AMONG OTHER PROVISIONS, THE LICENSE, THE DISCLAIMER OF WARRANTY AND THE LIMITATION OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT OR ARE NOT AUTHORIZED TO ENTER INTO THIS AGREEMENT, ENTERASYS IS UNWILLING TO LICENSE THE PROGRAM TO YOU AND YOU AGREE TO RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS, LEGAL DEPARTMENT AT (603) 332-9400.

You and Enterasys agree as follows:

1. LICENSE. You have the non-exclusive and non-transferable right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this Agreement.

2. RESTRICTIONS. Except as otherwise authorized in writing by Enterasys, You may not, nor may You permit any third party to:

(i) Reverse engineer, decompile, disassemble or modify the Program, in whole or in part, including for reasons of error correction or interoperability, except to the extent expressly permitted by applicable law and to the extent the parties shall not be permitted by that applicable law, such rights are expressly excluded. Information necessary to achieve interoperability or correct errors is available from Enterasys upon request and upon payment of Enterasys' applicable fee.

(ii) Incorporate the Program, in whole or in part, in any other product or create derivative works based on the Program, in whole or in part.

(iii) Publish, disclose, copy, reproduce or transmit the Program, in whole or in part.

(iv) Assign, sell, license, sublicense, rent, lease, encumber by way of security interest, pledge or otherwise transfer the Program, in whole or in part, except for a sale or other transfer of the hardware in which the Program is embedded.

(v) Remove any copyright, trademark, proprietary rights, disclaimer or warning notice included on or embedded in any part of the Program.

3. APPLICABLE LAW. This Agreement shall be interpreted and governed under the laws and in the state and federal courts of New Hampshire without regard to its conflicts of laws provisions. You accept the personal jurisdiction and venue of the New Hampshire courts. None of the 1980 United Nations Convention on Contracts for the International Sale of Goods, the United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

4. EXPORT RESTRICTIONS. You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the Program is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Sections 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, Cuba, Estonia, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Latvia, Libya, Lithuania, Moldova, North Korea, the People's Republic of China, Romania, Russia, Rwanda, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant or any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

5. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The enclosed Program (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Program is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the Government is subject to restrictions set forth herein.

6. DISCLAIMER OF WARRANTY. ENTERASYS DISCLAIMS ALL WARRANTIES, OTHER THAN THOSE SUPPLIED TO YOU BY ENTERASYS IN WRITING, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON- INFRINGEMENT WITH RESPECT TO THE PROGRAM. IF IMPLIED WARRANTIES MAY NOT BE DISCLAIMED BY APPLICABLE LAW, THEN ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THIRTY (30) DAYS AFTER DELIVERY OF THE PROGRAM TO YOU.

7. LIMITATION OF LIABILITY. IN NO EVENT SHALL ENTERASYS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM, EVEN IF ENTERASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS FOREGOING LIMITATION SHALL APPLY REGARDLESS OF THE CAUSE OF ACTION UNDER WHICH DAMAGES ARE SOUGHT.

THE CUMULATIVE LIABILITY OF ENTERASYS TO YOU FOR ALL CLAIMS RELATING TO THE PROGRAM, IN CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE TOTAL AMOUNT OF FEES PAID TO ENTERASYS BY YOU FOR THE RIGHTS GRANTED HEREIN.

8. AUDIT RIGHTS. You hereby acknowledge that the intellectual property rights associated with the Program are of critical value to Enterasys and, accordingly, You hereby agree to maintain complete books, records and accounts showing (i) license fees due and paid, and (ii) the use, copying and deployment of the Program. You also grant to Enterasys and its authorized representatives, upon reasonable notice, the right to audit and examine during Your normal business hours, Your books, records, accounts and hardware devices upon which the Program may be deployed to verify compliance with this Agreement, including the verification of the license fees due and paid Enterasys and the use, copying and deployment of the Program. Enterasys' right of examination shall be exercised reasonably, in good faith and in a manner calculated to not unreasonably interfere with Your business. In the event such audit discovers non-compliance with this Agreement, including copies of the Program made, used or deployed in breach of this Agreement, You shall promptly pay to Enterasys the appropriate license fees. Enterasys reserves the right, to be exercised in its sole discretion and without prior notice, to terminate this license, effective immediately, for failure to comply with this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

9. OWNERSHIP. This is a license agreement and not an agreement for sale. You acknowledge and agree that the Program constitutes trade secrets and/or copyrighted material of Enterasys and/or its suppliers. You agree to implement reasonable security measures to protect such trade secrets and copyrighted material. All right, title and interest in and to the Program shall remain with Enterasys and/or its suppliers. All rights not specifically granted to You shall be reserved to Enterasys.

10. ENFORCEMENT. You acknowledge and agree that any breach of Sections 2, 4, or 9 of this Agreement by You may cause Enterasys irreparable damage for which recovery of money damages would be inadequate, and that Enterasys may be entitled to seek timely injunctive relief to protect Enterasys' rights under this Agreement in addition to any and all remedies available at law.

11. ASSIGNMENT. You may not assign, transfer or sublicense this Agreement or any of Your rights or obligations under this Agreement, except in connection with the sale or other transfer of the hardware in which the Program is embedded. Enterasys may assign this Agreement in its sole discretion.

12. WAIVER. A waiver by Enterasys of a breach of any of the terms and conditions of this Agreement must be in writing and will not be construed as a waiver of any subsequent breach of such term or condition. Enterasys' failure to enforce a term upon Your breach of such term shall not be construed as a waiver of Your breach or prevent enforcement on any other occasion.

13. SEVERABILITY. In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired thereby, and that provision shall be reformed, construed and enforced to the maximum extent permissible. Any such invalidity, illegality or unenforceability in any jurisdiction shall not invalidate or render illegal or unenforceable such provision in any other jurisdiction.

14. TERMINATION. Enterasys may terminate this Agreement immediately upon Your breach of any of the terms and conditions of this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

Contents

Figures xii
Tables.. xv

ABOUT THIS GUIDE

Using This guide xvii
Structure of This Guide xviii
Related Documents... xx
Document Conventions... xx
Typographical and Keystroke Conventions.. xxi

1 INTRODUCTION

1.1 Overview 1-1
1.1.1 The Management Agent 1-2
1.1.2 In-Band vs. Out-of-Band 1-3
1.2 Navigating Local Management Screens 1-3
1.3 Local Management Requirements 1-3
1.4 Local Management Screen Elements 1-4
1.5 Local Management Keyboard Conventions 1-6
1.6 Getting Help 1-7

2 LOCAL MANAGEMENT REQUIREMENTS

2.1 Management Terminal Setup.. 2-1
2.1.1 Console Cable Connection 2-2
2.1.2 Management Terminal Setup Parameters.................................. 2-3
2.2 Telnet Connections 2-4
2.3 Monitoring an Uninterruptible Power Supply...................................... 2-4

3 ACCESSING LOCAL MANAGEMENT

3.1 Navigating Local Management Screens 3-1
3.1.1 Selecting Local Management Menu Screen Items 3-3
3.1.2 Exiting Local Management Screens 3-3
3.1.3 Using the NEXT and PREVIOUS Commands 3-4
3.1.4 Using the CLEAR COUNTERS Command.................................. 3-4
3.2 Password Screen.. 3-4

3.3 Device Menu Screen ... 3-7
3.4 Overview of Security Methods ... 3-11
3.4.1 Host Access Control Authentication (HACA) ... 3-12
3.4.2 802.1X Port Based Network Access Control ... 3-15
3.4.2.1 Definitions of Terms and Abbreviations ... 3-15
3.4.2.2 802.1X Security Overview ... 3-16
3.4.3 MAC Authentication Overview ... 3-17
3.4.3.1 Authentication Method Selection ... 3-17
3.4.3.2 Authentication Method Sequence ... 3-17
3.4.3.3 Concurrent Operation of 802.1X and MAC Authentication ... 3-18
3.4.4 MAC Authentication Control ... 3-21
3.5 Security Menu Screen ... 3-22
3.6 Passwords Screen ... 3-25
3.6.1 Setting the Module Login Password ... 3-27
3.7 Radius Configuration Screen ... 3-27
3.7.1 Setting the Last Resort Authentication ... 3-30
3.7.2 Setting the Local and Remote Servers ... 3-30
3.8 Name Services Configuration Screen ... 3-31
3.9 System Authentication Configuration Screen ... 3-33
3.10 EAP (Port) Configuration Screen ... 3-35
3.11 EAP Statistics Menu Screen ... 3-40
3.11.1 EAP Session Statistics Screen ... 3-42
3.11.2 EAP Authenticator Statistics Screen ... 3-44
3.11.3 EAP Diagnostic Statistics Screen ... 3-47
3.12 MAC Port Configuration Screen ... 3-50
3.13 MAC Supplicant Configuration Screen ... 3-52

4 DEVICE CONFIGURATION MENU SCREENS

4.1 Device Configuration Menu Screen ... 4-2
4.2 General Configuration Screen ... 4-4
4.2.1 Setting the IP Address ... 4-8
4.2.2 Setting the Subnet Mask ... 4-9
4.2.3 Setting the Default Gateway ... 4-10
4.2.4 Setting the TFTP Gateway IP Address ... 4-10
4.2.5 Setting the Module Name ... 4-11
4.2.6 Setting the Device Date ... 4-11
4.2.7 Setting the Device Time ... 4-12
4.2.8 Entering a New Screen Refresh Time ... 4-12
4.2.9 Setting the Screen Lockout Time ... 4-12
4.2.10 Configuring the COM Port ... 4-13
4.2.10.1 Changing the COM Port Application ... 4-14
4.2.11 Clearing NVRAM ... 4-15
4.2.12 Enabling/Disabling IP Fragmentation ... 4-16

4.3 SNMP Configuration Menu Screen 4-17
4.4 SNMP Community Names Configuration Screen 4-18
4.4.1 Establishing Community Names 4-20
4.5 SNMP Traps Configuration Screen 4-21
4.5.1 Configuring the Trap Table 4-22
4.6 Access Control List Screen 4-23
4.6.1 Entering IP Addresses 4-25
4.6.2 Enable/Disable ACL 4-27
4.7 System Resources Information Screen 4-28
4.7.1 Setting the Reset Peak Switch Utilization 4-29
4.8 FLASH Download Configuration Screen 4-30
4.8.1 Image File Download Using Runtime 4-34
4.8.2 Configuration File Download Using TFTP 4-34
4.8.3 Configuration File Upload Using TFTP 4-35

5 PORT CONFIGURATION MENU SCREENS

5.1 Port Configuration Menu Screen 5-2
5.2 Ethernet Interface Configuration Screen 5-4
5.3 Ethernet Port Configuration Screen 5-7
5.3.1 Selecting Field Settings 5-12
5.3.2 Setting the Advertised Ability 5-12
5.4 HSIM/VHSIM Configuration Screen 5-13
5.5 Redirect Configuration Menu Screen 5-13
5.6 Port Redirect Configuration Screen 5-15
5.6.1 Changing Source and Destination Ports 5-18
5.7 VLAN Redirect Configuration Screen 5-19
5.7.1 Changing Source VLAN and Destination Ports 5-22
5.8 Link Aggregation Menu Screen (802.3ad Main Menu Screen) 5-23
5.8.1 802.3ad Port Screen 5-27
5.8.1.1 802.3ad Port Details Screen 5-30
5.8.1.2 802.3ad Port Statistics Screen 5-36
5.8.2 802.3ad Aggregator Screen 5-39
5.8.2.1 802.3ad Aggregator Details Screen 5-41
5.8.3 802.3ad System Screen 5-43
5.9 Broadcast Suppression Configuration Screen 5-44
5.9.1 Setting the Threshold 5-46
5.9.2 Setting the Reset Peak 5-46

6 802.1 CONFIGURATION MENU SCREENS

6.1 802.1 Configuration Menu Screen 6-2
6.2 Spanning Tree Configuration Menu Screen 6-4
6.3 Spanning Tree Configuration Screen 6-5
6.3.1 Configuring a VLAN Spanning Tree 6-8
6.4 Spanning Tree Port Configuration Screen 6-9
6.4.1 Enabling/Disabling the Default Spanning Tree Ports 6-11
6.4.2 Viewing Status of Spanning Tree Ports 6-11
6.5 PVST Port Configuration Screen 6-11

7 802.1Q VLAN CONFIGURATION MENU SCREENS

7.1 Summary of VLAN Local Management 7-2
7.1.1 Preparing for VLAN Configuration 7-2
7.2 802.1Q VLAN Configuration Menu Screen 7-3
7.3 Static VLAN Configuration Screen 7-6
7.3.1 Creating a Static VLAN 7-8
7.3.2 Displaying the Current Static VLAN Port Egress List 7-9
7.3.3 Renaming a Static VLAN 7-9
7.3.4 Deleting a Static VLAN 7-10
7.3.5 Paging Through the VLAN List 7-10
7.4 Static VLAN Egress Configuration Screen 7-11
7.4.1 Setting Egress Types on Ports 7-13
7.4.2 Displaying the Next Group of Ports 7-14
7.5 Current VLAN Configuration Screen 7-14
7.6 Current VLAN Egress Configuration Screen 7-16
7.7 VLAN Port Configuration Screen 7-17
7.7.1 Changing the Port Mode 7-20
7.7.2 Configuring the VLAN Ports 7-20
7.8 VLAN Classification Configuration Screen 7-21
7.8.1 Classification Precedence Rules 7-29
7.8.2 Displaying the Current Classification Rule Assignments 7-32
7.8.3 Assigning a Classification to a VID 7-33
7.8.4 Deleting Line Items 7-34
7.9 Protocol Port Configuration Screen 7-34
7.9.1 Assigning Ports to a VID/Classification 7-37

8 802.1p CONFIGURATION MENU SCREENS

8.1 802.1p Configuration Menu Screen 8-2
8.2 Port Priority Configuration Screen 8-4
8.2.1 Setting Switch Port Priority Port-by-Port 8-6
8.2.2 Setting Switch Port Priority on All Ports 8-7
8.3 Traffic Class Information Screen 8-7
8.4 Traffic Class Configuration Screen 8-10
8.4.1 Assigning the Traffic Class to Port Priority 8-11
8.5 Transmit Queues Configuration Screen 8-12
8.5.1 Setting the Current Queueing Mode 8-15
8.6 Priority Classification Configuration Screen 8-16
8.6.1 Classification Precedence Rules 8-26
8.6.2 About the IP TOS Rewrite Function 8-29
8.6.3 Displaying the Current PID/Classification Assignments 8-30
8.6.4 Assigning a Classification to a PID 8-30
8.6.5 Deleting PID/Classification/Description Line Items 8-31
8.7 Protocol Port Configuration Screen 8-32
8.7.1 Assigning Ports to a PID/Classification 8-34
8.7.2 Solving the Problem 8-35
8.8 Rate Limiting Configuration Screen 8-37
8.8.1 Configuring a Port 8-41
8.8.2 Changing/Deleting Port Line Items 8-43
8.8.3 More About Rate Limiting 8-44

9 LAYER 3 EXTENSIONS MENU SCREENS

9.1 Layer 3 Extensions Menu Screen 9-1
9.2 IGMP/VLAN Configuration Screen 9-3
9.2.1 IGMP/VLAN Configuration Procedure 9-7

10 DEVICE STATISTICS MENU SCREENS

10.1 Device Statistics Menu Screen 10-1
10.2 Switch Statistics Screen 10-3
10.3 Interface Statistics Screen 10-5
10.3.1 Displaying Interface Statistics 10-8
10.4 RMON Statistics Screen 10-9
10.4.1 Displaying RMON Statistics 10-12

11 NETWORK TOOLS SCREENS

11.1 Network Tools 11-1
11.2 Built-in Commands 11-4
11.3 Example, Effects of Aging Time on Dynamic Egress 11-39
11.4 Example, Using Dynamic Egress to Control Traffic 11-39
11.5 Special Commands 11-40

12 VLAN OPERATION AND NETWORK APPLICATIONS

12.1 Defining VLANs 12-2
12.2 Types of VLANs 12-3
12.2.1 802.1Q VLANs 12-3
12.2.2 Other VLAN Strategies 12-3
12.3 Benefits and Restrictions 12-4
12.4 VLAN Terms 12-4
12.5 VLAN Operation 12-7
12.5.1 Description 12-7
12.5.2 VLAN Components 12-7
12.6 Configuration Process 12-7
12.6.1 Defining a VLAN 12-8
12.6.2 Classifying Frames to a VLAN 12-8
12.6.3 Customizing the VLAN Forwarding List 12-8
12.7 VLAN Switch Operation 12-8
12.7.1 Receiving Frames from VLAN Ports 12-10
12.7.2 Forwarding Decisions 12-10
12.7.2.1 Broadcasts, Multicasts, and Unknown Unicasts 12-10
12.7.2.2 Known Unicasts 12-11
12.8 VLAN Configuration 12-11
12.8.1 Managing the Switch 12-11
12.8.2 Switch Without VLANs 12-12
12.8.3 Switch with VLANs 12-12
12.9 Summary of VLAN Local Management 12-15
12.9.1 Preparing for VLAN Configuration 12-15
12.10 Quick VLAN Walkthrough 12-16
12.11 Examples 12-21
12.12 Example 1, Single Switch Operation 12-21
12.12.1 Solving the Problem 12-22
12.12.2 Frame Handling 12-23
12.13 Example 2, VLANs Across Multiple Switches 12-24
12.13.1 Solving the Problem 12-26
12.13.2 Frame Handling 12-29

12.14 Example 3, Filtering Traffic According to a Layer 4 Classification Rule...... 12-32
12.14.1 Solving the Problem.. 12-32
12.15 Example 4, Securing Sensitive Information According to Subnet............... 12-33
12.15.1 Solving the Problem.. 12-34
12.16 Example 5, Using Dynamic Egress to Control Traffic 12-34
12.17 Example 6, Locking a MAC Address to a Port Using Classification Rules . 12-36
12.17.1 Solving the Problem.. 12-36

A GENERIC ATTRIBUTE REGISTRATION PROTOCOL (GARP)

A.1 Overview A-1
A.2 How It Works...A-2

B ABOUT IGMP

B.1 IGMP Overview B-1
B.2 Supported Features and Functions...B-2
B.3 Detecting Multicast Routers B-3

INDEX

Figures

Figure Page

1-1 Example of a Local Management Screen 1-4
2-1 Management Terminal Connection 2-2
2-2 Uninterruptible Power Supply (UPS) Connection 2-5
3-1 802.1Q Switching Mode, LM Screen Hierarchy 3-2
3-2 Local Management Password Screen 3-5
3-3 Device Menu Screen 3-7
3-4 Security Menu Screen 3-23
3-5 Module Login Passwords Screen 3-25
3-6 Radius Configuration Screen 3-28
3-7 Name Services Configuration Screen 3-31
3-8 System Authentication Configuration Screen 3-33
3-9 EAP Port Configuration Screen 3-35
3-10 EAP Statistics Menu Screen 3-40
3-11 EAP Session Statistics Screen 3-42
3-12 EAP Authenticator Statistics Screen 3-45
3-13 EAP Diagnostic Statistics Screen 3-47
3-14 MAC Port Configuration Screen 3-51
3-15 MAC Supplicant Configuration Screen 3-53
4-1 Device Configuration Menu Screen 4-2
4-2 General Configuration Screen 4-4
4-3 Configuration Warning Screen, IP Address 4-8
4-4 Configuration Warning Screen, Subnet Mask 4-9
4-5 COM Port Warning 4-14
4-6 Clear NVRAM Warning 4-16
4-7 SNMP Configuration Menu Screen 4-17
4-8 SNMP Community Names Configuration Screen 4-19
4-9 SNMP Traps Configuration Screen 4-21
4-10 Access Control List Screen 4-23
4-11 System Resources Information Screen 4-28
4-12 Flash Download Configuration Screen 4-31
5-1 Port Configuration Menu Screen (in Agg Mode, HUNTGROUP) 5-2
5-2 Port Configuration Menu Screen (in Agg Mode, IEEE8023ad) 5-3
5-3 Ethernet Interface Configuration Screen 5-5
5-4 Ethernet Port Configuration Screen 5-8
5-5 Redirect Configuration Menu Screen 5-14
5-6 Port Redirect Configuration Screen 5-16

Figure Page

5-7 VLAN Redirect Configuration Screen 5-20
5-8 802.3ad Main Menu Screen 5-26
5-9 802.3ad Port Screen 5-28
5-10 802.3ad Port Details Screen 5-30
5-11 802.3ad Port Statistics Screen 5-36
5-12 802.3ad Aggregator Screen 5-39
5-13 802.3ad Aggregator Details Screen 5-41
5-14 802.3ad System Screen 5-43
5-15 Broadcast Suppression Configuration Screen 5-45
6-1 802.1 Configuration Menu Screen 6-2
6-2 Spanning Tree Configuration Menu Screen 6-4
6-3 Spanning Tree Configuration Screen 6-6
6-4 Spanning Tree Port Configuration Screen 6-9
6-5 PVST Port Configuration Screen 6-12
7-1 802.1Q VLAN Screen Hierarchy 7-2
7-2 802.1Q VLAN Configuration Menu Screen 7-4
7-3 Static VLAN Configuration Screen 7-7
7-4 Static VLAN Egress Configuration Screen 7-11
7-5 Current VLAN Configuration Screen 7-15
7-6 Current VLAN Egress Configuration Screen 7-16
7-7 VLAN Port Configuration Screen 7-18
7-8 VLAN Classification Configuration Screen 7-22
7-9 Protocol Port Configuration Screen 7-35
8-1 802.1p Configuration Menu Screen 8-2
8-2 Port Priority Configuration Screen 8-5
8-3 Traffic Class Information Screen 8-8
8-4 Traffic Class Configuration Screen 8-10
8-5 Transmit Queues Configuration Screen 8-13
8-6 Priority Classification Configuration Screen 8-17
8-7 Datagram, Layer 2 and Layer 3 8-29
8-8 Protocol Port Configuration Screen 8-32
8-9 Prioritizing Network Traffic According to Classification Rule 8-35
8-10 Rate Limiting Configuration Screen 8-38
9-1 Layer 3 Extensions Menu Screen 9-2
9-2 IGMP/VLAN Configuration Screen 9-4
10-1 Device Statistics Menu Screen 10-2
10-2 Switch Statistics Screen 10-4
10-3 Interface Statistics Screen 10-6
10-4 RMON Statistics Screen 10-9
11-1 Example, Dynamic Egress Application 11-39
12-1 Example of a VLAN 12-2
12-2 View from Inside the Switch 12-9

Figure Page

12-3 Switch Management with Only Default VLAN 12-12
12-4 Switch Management with VLANs 12-13
12-5 802.1Q VLAN Screen Hierarchy 12-15
12-6 Walkthrough Stage One, Static VLAN Configuration Screen 12-17
12-7 Walkthrough Stage Two, Port 3 Egress Setting 12-18
12-8 Walkthrough Stage Three, Port 10 Egress Setting 12-19
12-9 Walkthrough Stage Four, VLAN Port Configuration 12-20
12-10 Example 1, Single Switch Operation 12-21
12-11 Switch Configured for VLANs 12-23
12-12 Example 2, VLANs Across Multiple Switches 12-25
12-13 Bridge 1 Broadcasts Frames 12-29
12-14 Transmitting to Switch 4 12-30
12-15 Transmitting to Bridge 4 12-31
12-16 Example 3, Filtering Traffic According to a Classification 12-32
12-17 Example 4, Securing Traffic to One Subnet 12-33
12-18 Example 5, Dynamic Egress Application 12-35
12-19 Example 6, Locking Ports According to Classification Rule 12-36
A-1 Example of VLAN Propagation via GVRP A-2

Tables

Table Page

1-1 Event Messages 5
1-2 Keyboard Conventions 6
2-1 VT Terminal Setup 3
3-1 Device Menu Screen Menu Item Descriptions 8
3-2 Authentication Terms and Abbreviations 15
3-3 MAC / 802.1X Precedence States 19
3-4 Security Menu Screen Menu Item Descriptions 24
3-5 Module Login Passwords Screen Field Descriptions 26
3-6 Radius Configuration Screen Field Descriptions 28
3-7 Name Services Configuration Screen Field Descriptions 32
3-8 System Authentication Configuration Screen Field Descriptions 34
3-9 EAP Port Configuration Screen Field Descriptions 36
3-10 EAP Statistics Menu Screen Descriptions 41
3-11 EAP Session Statistics Screen Field Descriptions 43
3-12 EAP Authenticator Statistics Screen Field Descriptions 45
3-13 EAP Diagnostic Statistics Screen Field Descriptions 48
3-14 MAC Port Configuration Screen Field Descriptions 51
3-15 MAC Supplicant Configuration Screen Field Descriptions 53
4-1 Device Configuration Menu Screen Menu Item Descriptions 3
4-2 General Configuration Screen Field Descriptions 5
4-3 COM Port Application Settings 15
4-4 SNMP Configuration Menu Screen Menu Item Descriptions 18
4-5 SNMP Community Names Configuration Screen Field Descriptions 19
4-6 SNMP Traps Configuration Screen Field Descriptions 22
4-7 Access Control List Screen Field Descriptions 24
4-8 System Resources Information Screen Field Descriptions 29
4-9 Flash Download Configuration Screen Field Descriptions 32
5-1 Port Configuration Menu Screen Menu Item Descriptions 3
5-2 Ethernet Interface Configuration Screen Field Descriptions 5
5-3 Ethernet Port Configuration Screen Field Descriptions 9
5-4 Redirect Configuration Menu Screen Menu Item Descriptions 14
5-5 Port Redirect Configuration Screen Field Descriptions 16
5-6 VLAN Redirect Configuration Screen Field Descriptions 21
5-7 802.3ad Main Menu Screen Menu Item Descriptions 27
5-8 802.3ad Port Screen Field Descriptions 29
5-9 802.3ad Port Details Screen Field Descriptions 31
5-10 802.3ad Port Statistics Screen Field Descriptions 37

Table Page

5-11 802.3ad Aggregator Screen Field Descriptions 40
5-12 802.3ad Aggregator Details Screen Field Descriptions 42
5-13 802.3ad System Screen Field Descriptions 44
5-14 Broadcast Suppression Configuration Screen Field Descriptions 45
6-1 802.1 Configuration Menu Screen Menu Item Descriptions 3
6-2 Spanning Tree Configuration Menu Screen...5
6-3 Spanning Tree Configuration Screen...6
6-4 Spanning Tree Port Configuration Screen 10
6-5 PVST Port Configuration Screen Field Descriptions..12
7-1 802.1Q VLAN Configuration Menu Screen Menu Item Descriptions 5
7-2 Static VLAN Configuration Screen Field Descriptions 7
7-3 Static VLAN Egress Configuration Screen Field Descriptions 12
7-4 Current VLAN Configuration Screen Field Descriptions 15
7-5 Current VLAN Egress Configuration Screen Field Descriptions 17
7-6 VLAN Port Configuration Screen Field Descriptions..18
7-7 VLAN Classification Configuration Screen Field Descriptions 22
7-8 Classification List 24
7-9 Classification Precedence...30
7-10 Protocol Port Configuration Screen Field Descriptions..36
8-1 802.1p Configuration Menu Screen Menu Item Descriptions 3
8-2 Port Priority Configuration Screen Field Descriptions..6
8-3 Traffic Class Information Screen Field Descriptions 9
8-4 Traffic Class Configuration Screen Field Descriptions..11
8-5 Transmit Queues Configuration Screen Field Descriptions 14
8-6 Priority Classification Configuration Screen Field Descriptions 17
8-7 Classification List 19
8-8 Classification Precedence...27
8-9 Protocol Port Configuration Screen Field Descriptions..33
8-10 Rate Limiting Configuration Screen Field Descriptions...38
9-1 Layer 3 Extensions Menu Screen Menu Item Descriptions 2
9-2 IGMP/VLAN Configuration Screen Field Descriptions 4
10-1 Device Statistics Menu Screen Menu Item Descriptions 2
10-2 Switch Statistics Screen Field Descriptions 4
10-3 Interface Statistics Screen Field Descriptions...6
10-4 RMON Statistics Screen Field Descriptions...10
11-1 Built-In Commands 3
11-2 Path Cost Parameter Values 32
12-1 VLAN Terms and Definitions...4

About This Guide

Welcome to the Enterasys Networks ***SmartSwitch 2200 Series (2E253, 2H252, 2H253, and 2H258) Standalone Switches Local Management User's Guide***. This manual explains how to access and use the Enterasys Networks Local Management to manage the SmartSwitch devices. Local Management is a series of screens that enable the user to monitor and control the SmartSwitch device and its attached segments.

Important Notice

Depending on the firmware version used in the SmartSwitch device, some features described in this document may not be supported. Refer to the Release Notes shipped with the SmartSwitch device to determine which features are supported.

USING THIS GUIDE

A general working knowledge of basic network operations and an understanding of management applications is helpful before using Local Management.

This manual describes how to do the following:

- Access the Local Management application
- Identify and operate the types of fields used by Local Management
- Navigate through Local Management fields and menus
- Use Local Management screens to perform management operations
- Establish and manage Virtual Local Area Networks (VLANs)

STRUCTURE OF THIS GUIDE

The guide is organized as follows:

Chapter 1, **Introduction**, provides an overview of the tasks that may be accomplished using Local Management (LM), and an introduction to LM screen navigation, in-band and out-of-band network management, screen elements, and LM keyboard conventions.

Chapter 2, **Local Management Requirements**, provides the setup requirements for accessing Local Management, the instructions to configure and connect a management terminal to the SmartSwitch device, and the instructions for connecting the SmartSwitch device to an Uninterruptible Power Supply (UPS) for monitoring the UPS power status.

Chapter 3, **Accessing Local Management**, describes how to access the Main Menu screen and navigate the Local Management screens. This chapter also describes the security screens.

Chapter 4, **Device Configuration Menu Screens**, describes the Device Configuration Menu screen and the screens that can be selected from it. These screens are used to control access to the SmartSwitch device by assigning community names, configure the SmartSwitch device to send SNMP trap messages to multiple network management stations, limit access according to an Access Control List (ACL) for additional security, access system resource information, download a new firmware image to the switch module, provide access to menu screens to configure ports, and configure the switch module for 802.1, 802.1Q VLAN, and layer 3 operations.

Chapter 5, **Port Configuration Menu Screens**, describes how to use the screens to configure the ports for various operations, such as for Ethernet Interface, HSIM/VHSIM, port and VLAN redirect, SmartTrunk, and broadcast suppressor configuration.

Chapter 6, **802.1 Configuration Menu Screens**, describes how to access the Spanning Tree Configuration Menu, 802.1Q VLAN Configuration Menu, and 802.1p Configuration Menu, screens. This chapter also introduces and describes how to use the Spanning Tree screens to create a separate Spanning Tree topology for each VLAN configured in the SmartSwitch device.

Chapter 7, **802.1Q VLAN Configuration Menu Screens**, describes how to use the screens to create static VLANs, select the mode of operation for each port, filter frames according to VLAN, establish VLAN forwarding (Egress) lists, route frames according to VLAN ID, display the current ports and port types associated with a VLAN and protocol, and configure ports on the switch as GVRP-aware ports. VLAN classification and classification rules are also discussed.

Chapter 8, **802.1p Configuration Menu Screens**, describes how to use the screens to set the transmit priority of each port, display the current traffic class mapping-to-priority of each port, set ports to either transmit frames according to selected priority transmit queues or percentage of port transmission capacity for each queue, assign transmit priorities according to protocol types, and configure a rate limit for a given port and list of priorities.

Chapter 9, **Layer 3 Extensions Menu Screens**, introduces and describes how to enable or disable IGMP (Internet Group Management Protocol, RFC 2236) on selected VLANs, or globally on all VLANs that are available.

Chapter 10, **Device Statistics Menu Screens**, introduces and describes how to use the statistics screens to gather statistics about the switch, interfaces, RMON, and HSIM/VHSIM and, if the device is a repeater, repeater statistics.

Chapter 11, **Network Tools Screens**, describes how to access and use the Network Tools screens. This chapter also lists built-in and new functional CLI commands, including examples.

Chapter 12, **VLAN Operation and Network Applications**, introduces VLANs, describes how they operate, and how to configure them using the Local Management screens described in Chapter 7. Examples are also provided to show how VLANs are configured to solve a problem and how the VLAN frames travel through the network.

Appendix A, **Generic Attribute Registration Protocol (GARP)**, describes the switch operation when its ports are configured to operate under the Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) application.

NOTE: There is a global setting for GVRP that is enabled by default. However, this setting is only accessible through a Management Information Base (MIB).

Appendix B, **About IGMP**, introduces the Internet Group Management Protocol (IGMP), its features and functions, and describes how it detects multicast routers.

RELATED DOCUMENTS

The following Enterasys Networks documents may help to set up, control, and manage the SmartSwitch device:

- *Ethernet Technology Guide*
- *Cabling Guide*
- *SmartTrunk User's Guide*
- *WAN Series Local Management User's Guide*

Documents associated with the optional HSIM and VHSIM interface modules, SmartSwitch device installation user's guides, and the manuals listed above, can be obtained from the World Wide Web in Adobe Acrobat Portable Document Format (PDF) at the following web site:

http://www.enterasys.com/

DOCUMENT CONVENTIONS

This guide uses the following conventions:

NOTE: Calls the reader's attention to any item of information that may be of special importance.

TIP: Conveys helpful hints concerning procedures or actions.

CAUTION: Contains information essential to avoid damage to the equipment.

TYPOGRAPHICAL AND KEYSTROKE CONVENTIONS

bold type Bold type can denote either a user input or a highlighted screen selection.

RETURN Indicates either the ENTER or RETURN key, depending on your keyboard.

ESC Indicates the keyboard Escape key.

SPACE bar Indicates the keyboard space bar key.

BACKSPACE Indicates the keyboard backspace key.

arrow keys Refers to the four keyboard arrow keys.

[-] Indicates the keyboard – key.

DEL Indicates the keyboard delete key.

italic type Italic type indicates complete document titles.

n.nn A period in numerals signals the decimal point indicator (e.g., 1.75 equals one and three fourths). Or, periods used in numerals signal the decimal point in Dotted Decimal Notation (DDN) (e.g., 000.000.000.000 in an IP address).

x A lowercase italic *x* indicates the generic use of a letter (e.g., *xxx* indicates any combination of three alphabetic characters).

n A lowercase italic *n* indicates the generic use of a number (e.g., 19*nn* indicates a four-digit number in which the last two digits are unknown).

[ ] In the Local Management screens, the square brackets indicate that a value may be selected. In the format descriptions in the Network Tools section, required arguments are enclosed in square brackets, [ ].

< > In the format descriptions in the Network Tools section, optional arguments are enclosed in angle brackets, < >.

1

Introduction

This chapter provides an overview of the tasks that may be accomplished using Local Management (LM), and an introduction to LM screen navigation, in-band and out-of-band network management, screen elements, and LM keyboard conventions.

Important Notice

Depending on the firmware version used in the SmartSwitch device, some features described in this document may not be supported. Refer to the Release Notes shipped with the SmartSwitch device to determine which features are supported.

1.1 OVERVIEW

Enterasys Networks' Local Management is a management tool that allows a network manager to perform the following tasks:

- Assign IP address and subnet mask.
- Select a default gateway.
- Assign a login password to the device for additional security.
- Download a new firmware image.
- Upload or download a configuration file to or from a TFTP server.
- Designate which Network Management Workstations receive SNMP traps from the device.
- View switch, interface, and RMON statistics.
- Assign ports to operate in the standard or full duplex mode.
- Configure ports to perform load sharing using SmartTrunking. Refer to the *SmartTrunk User's Guide* for details.
- Control the number of receive broadcasts that are switched to the other interfaces.
- Set flow control on a port-by-port basis.
- Configure ports to prioritize incoming frames at Layer 2, Layer 3, and Layer 4.

- Clear NVRAM.
- Set 802.1Q VLAN memberships and port configurations.
- Redirect frames according to port or VLAN and transmit them on a preselected destination port.
- Create a separate Spanning Tree topology for each VLAN configured in the SmartSwitch device.
- Transmit frames on preselected destination ports according to protocol and priority or protocol and VLAN.
- Configure the switch to operate as a Generic Attribute Registration Protocol (GARP) device to dynamically create VLANs across a switched network.
- Configure the device to control the rate of network traffic entering and leaving the switch on a per port/priority basis.
- Configure an optional HSIM or VHSIM installed in the device.
- Configure the device to dynamically switch frames according to a characteristic rule and VLAN.
- Configure ports on the SmartSwitch device as Router Redundancy Protocol (VRRP) ports.
- Provide additional security and policy administration capabilities via Port-based Web Authentication (PWA) by configuring pertinent variables within the LM screen.
- Configure multiple ports to act in an 802.3ad trunk group.
- Configure and manage the use of 802.1w, a standards-based method to rapidly fail over links to reduce downtime on a network.
- Provide additional security by configuring a physical port to lock on an attached device according to a Classification rule so no other device can be connected to that port and used.
- Configure the device to operate using the path cost values conforming legacy 802.1D or 802.1 standards.

There are three ways to access Local Management:

- Locally using a VT type terminal connected to the COM port.
- Remotely using a VT type terminal connected through a modem.
- In-band through a Telnet connection.

1.1.1 The Management Agent

The management agent is a process within the SmartSwitch device that collects statistical information (e.g., frames received, errors detected) about the operational performance of the managed network. Local Management communicates with the management agent for the purpose of viewing statistics or issuing management commands. Local Management provides a wide range of screens used to monitor and configure the SmartSwitch device.

1.1.2 In-Band vs. Out-of-Band

Network management systems are often classified as either in-band or out-of-band. In-band network management passes data along the same medium (cables, frequencies) used by all other stations on the network.

Out-of-band network management passes data along a medium that is entirely separate from the common data carrier of the network, for example, a cable connection between a dumb terminal and a SmartSwitch device COM port. The Enterasys Networks' Local Management is an out-of-band network management system.

A device connected out-of-band to the management agent is not connected to the LAN. This type of connection allows you to communicate with a network device even when that device is unable to communicate through the network, for example, at the time of installation.

1.2 NAVIGATING LOCAL MANAGEMENT SCREENS

To navigate within a Local Management screen, use the arrow keys of the terminal or the workstation providing terminal emulation services. The Local Management screen cursor responds to the LEFT, RIGHT, UP, and DOWN arrow keys. Each time you press an arrow key, the Local Management screen cursor moves to the next available field in the direction of the arrow key.

The Local Management screen cursor only moves to fields that can be selected or used for input. This means that the cursor jumps over display fields and empty lines on the Local Management screen.

The Local Management screen cursor provides wrap-around operation. This means that a cursor located at the edge of a screen, when moved in the direction of that edge, "wraps around" to the outermost selectable item on the opposite side of the screen which is on the same line or column.

1.3 LOCAL MANAGEMENT REQUIREMENTS

The SmartSwitch device provides one communication port, labeled COM, which supports a management terminal connection. To access Local Management, connect one of the following systems to the COM port:

- Digital Equipment Corporation VT series terminal.
- VT type terminal running emulation programs for the Digital Equipment Corporation VT series.
- IBM or compatible PC running a VT series emulation software package.

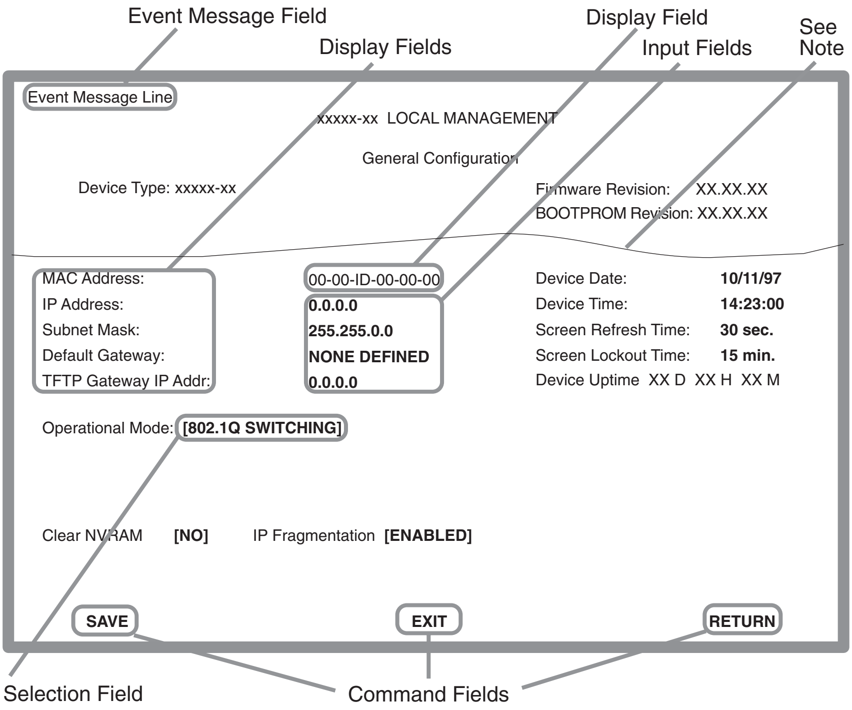
You can also access Local Management using a Telnet connection through one of the network ports of the SmartSwitch device.

NOTE: For details on the setup parameters for the console, how to connect a console to the SmartSwitch, or how to make a telnet connection, refer to Chapter 2.

1.4 LOCAL MANAGEMENT SCREEN ELEMENTS

There are six types of screens used in Local Management: password, menu, statistics, configuration, status, and warning screens. Each type of screen can consist of one to five basic elements, or fields. Figure 1-1 shows an example of the fields in a screen. A description of each field follows the figure.

Figure 1-1 Example of a Local Management Screen



```
Event Message Line
                         xxxxx-xx  LOCAL MANAGEMENT

                              General Configuration

        Device Type: xxxxx-xx                      Firmware Revision:     XX.XX.XX
                                                   BOOTPROM Revision: XX.XX.XX

  MAC Address:              00-00-ID-00-00-00      Device Date:           10/11/97
  IP Address:               0.0.0.0                Device Time:           14:23:00
  Subnet Mask:              255.255.0.0            Screen Refresh Time:   30 sec.
  Default Gateway:          NONE DEFINED           Screen Lockout Time:   15 min.
  TFTP Gateway IP Addr:     0.0.0.0                Device Uptime  XX D  XX H  XX M

  Operational Mode: [802.1Q SWITCHING]


  Clear NVRAM     [NO]     IP Fragmentation  [ENABLED]


      SAVE                        EXIT                        RETURN
```

Note: This shows the location of the cut away that is used in most of the screen graphics in this document. The top portion of the screen is cut away to eliminate repeating the same information in each graphic.The screen title is contained in its figure title.

30691_01

Event Message Field

This field briefly displays messages that indicate if a Local Management procedure was executed correctly or incorrectly, that changes were saved or not saved to Non-Volatile Random Access Memory (NVRAM), or that a user did not have access privileges to an application.

Table 1-1 describes the most common event messages. Event messages related to specific Local Management applications are described with those applications throughout this manual.

Table 1-1 Event Messages

Message	What it Means
SAVED OK	One or more fields were modified, and saved to NVRAM.
NOT SAVED --PRESS SAVE-- TO KEEP CHANGES	Attempting to exit the LM screen after one or more fields were modified, but not saved to NVRAM.
NOTHING TO SAVE	The SAVE command was executed, but nothing was saved to NVRAM because there were no configuration changes since the data was last saved.

Display Fields

Display fields cannot be edited. These fields may display information that never changes, or information that may change as a result of Local Management operations, user selections, or network monitoring information. In the screens shown in this guide, the characters in the display fields are in plain type (not bold). In the field description, the field is identified as being “read-only”.

Input Fields

Input Fields require the entry of keyboard characters. IP addresses, subnet mask, default gateway and device time are examples of input fields. In the screens shown in this guide, the characters in the input fields are in bold type. In the field description, the field is identified as being “modifiable”.

Selection Fields

Selection fields provide a series of possible values. Only applicable values appear in a selection field. In the screens shown in this guide, the selections display within brackets and are in **bold** type. In the field description, the field is identified as being either “selectable” when there are more than two possible values, or “toggle” when there are only two possible values.

Command Fields

Command fields (located at the bottom of Local Management screens) are used to exit Local Management screens, save Local Management entries, or navigate to another display of the same screen. In the screens shown in this guide, the characters in this field are all upper case and in bold type. In the field description, the field is identified as being a “command” field.

1.5 LOCAL MANAGEMENT KEYBOARD CONVENTIONS

All key names appear as capital letters in this manual. Table 1-2 explains the keyboard conventions and the key functions that are used.

Table 1-2 Keyboard Conventions

Key	Function
ENTER Key RETURN Key	Used to enter data or commands. These keys perform the same Local Management function. For example, “Press ENTER” means that you can press either ENTER or RETURN, unless this manual specifically instructs you otherwise.
ESCAPE (ESC) Key	Used to “escape” from a Local Management screen without saving changes. For example, “Press ESC twice” means the ESC key must be pressed quickly two times.
SPACE Bar BACKSPACE Key	Used to cycle through selections in some Local Management fields. Use the SPACE bar to cycle forward through selections and use the BACKSPACE key to cycle backward through selections.
Arrow Keys	(UP-ARROW, DOWN-ARROW, LEFT-ARROW, RIGHT-ARROW) Used to move the screen cursor. For example, “Use the arrow keys” means to press whichever arrow key moves the cursor to the desired field on the Local Management screen.
DEL Key	Used to remove characters from a Local Management field. For example, “Press DEL” means to press the Delete key.

1.6 GETTING HELP

For additional support related to this device or document, contact Enterasys Networks using one of the following methods:

World Wide Web	http://www.enterasys.com/
Phone	(603) 332-9400
Internet mail	support@enterasys.com
FTP	ftp://ftp.enterasys.com/
Login	*anonymous*
Password	*your email address*

To send comments or suggestions concerning this document, contact the Enterasys Networks Technical Writing Department via the following email address: **TechWriting@enterasys.com**

Make sure to include the document Part Number in the email message.

Before calling the Enterasys Networks, have the following information ready:

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (e.g., changing mode switches, rebooting the unit, etc.)
- The serial and revision numbers of all involved Enterasys Networks products in the network
- A description of your network environment (layout, cable type, etc.)
- Network load and frame size at the time of trouble (if known)
- The device history (i.e., have you returned the device before, is this a recurring problem, etc.)
- Any previous Return Material Authorization (RMA) numbers

2

Local Management Requirements

This chapter provides information concerning the following:

- Management Terminal Setup (Section 2.1), which describes how to attach a Local Management terminal to the Enterasys Networks host device.
- Telnet Connections (Section 2.2), which provides guidelines when using a Telnet connection to access Local Management.
- Monitoring an Uninterruptible Power Supply (Section 2.3), which describes how to make a connection from the COM port to an American Power Conversion (APC) Uninterruptible Power Supply (UPS) device. This type of connection enables the SmartSwitch device to monitor the power status in case of a power loss.

2.1 MANAGEMENT TERMINAL SETUP

Use one of the following systems to access Local Management:

- A PC or compatible device running a VT series emulation software package
- A Digital Equipment Corporation VT100 type terminal
- A VT type terminal running emulation programs for the Digital Equipment Corporation VT100 series
- A remote VT100 type terminal via a modem connection
- In-band via a Telnet connection

2.1.1 Console Cable Connection

Use the Console Cable Kit provided with the SmartSwitch device to attach the management terminal to the SmartSwitch device COM port as shown in Figure 2-1.

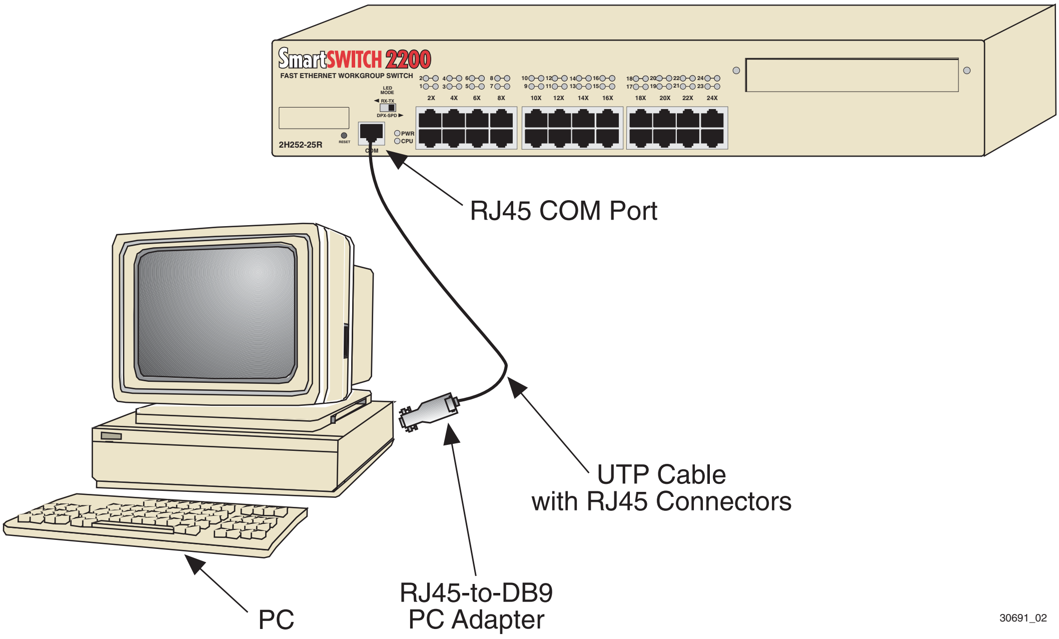
To connect the SmartSwitch device to a PC or compatible device running the VT terminal emulation, proceed as follows:

1. Connect the RJ45 connector at one end of the cable (supplied in the kit) to the COM port on the SmartSwitch device.
2. Plug the RJ45 connector at the other end of the cable into the RJ45-to-DB9 adapter (supplied in the kit).
3. Connect the RJ45-to-DB9 adapter to the communications port on the PC.

NOTE: If using a modem between the VT compatible device and the COM port of the SmartSwitch device, use the appropriate connector included in the console cable kit. Refer to the modem manufacturer's information for proper operation and setup of the modem.

The 2H252-25R SmartSwitch device is shown in Figure 2-1 as an example.

Figure 2-1 Management Terminal Connection



2.1.2 Management Terminal Setup Parameters

Table 2-1 lists the setup parameters for the local management terminal.

Table 2-1 VT Terminal Setup

Display Setup Menu	
Columns ->	80 Columns
Controls ->	Interpret Controls
Auto Wrap ->	No Auto Wrap
Scroll ->	Jump Scroll
Text Cursor ->	Cursor
Cursor Style ->	Underline Cursor Style
General Setup Menu	
Mode ->	VT100, 7 Bit Controls
ID number ->	VT100ID
Cursor Keys ->	Normal Cursor Keys
Power Supply ->	UPSS DEC Supplemental
Communications Setup Menu	
Transmit ->	2400, 4800, 9600, 19200
Receive ->	Receive=Transmit
XOFF ->	XOFF at 64
Bits ->	8 bits
Parity ->	No Parity
Stop Bit ->	1 Stop Bit
Local Echo ->	No Local Echo
Port ->	DEC-423, Data Leads Only
Transmit ->	Limited Transmit
Auto Answerback ->	No Auto Answerback
Keyboard Setup Menu	
Keys ->	Typewriter Keys
Auto Repeat ->	any option
Keyclick ->	any option
Margin Bell ->	Margin Bell
Warning Bell ->	Warning Bell

2.2 TELNET CONNECTIONS

Once the SmartSwitch device has a valid IP address, the user can establish a Telnet session from any TCP/IP based node on the network. Telnet connections to the SmartSwitch device require the community name passwords assigned in the SNMP Community Names Configuration screen.

For information about setting the IP address, refer to Section 4.2.

For information about assigning community names, refer to Section 4.4.

Refer to the instructions included with the Telnet application for information about establishing a Telnet session.

If the SmartSwitch device is operating in the 802.1Q mode with configured VLANs, the management station must be connected to a physical port on the device that is on the same VLAN as the virtual Host Data Port. For more information about the virtual Host Data Port and the setup information for remote management in a device that is to be configured with VLANs, refer to Section 12.8.

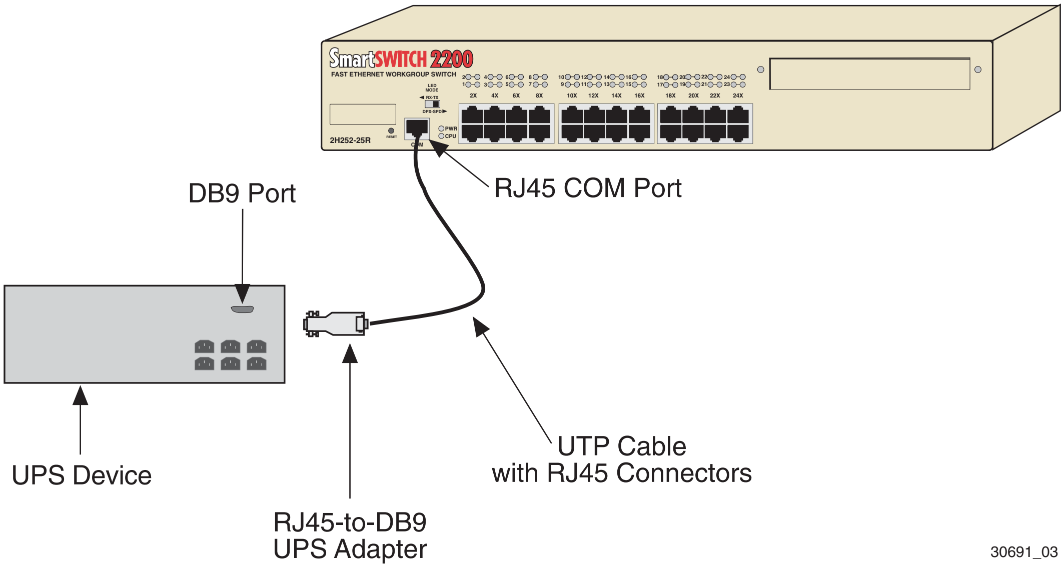
2.3 MONITORING AN UNINTERRUPTIBLE POWER SUPPLY

If the SmartSwitch device is connected to an American Power Conversion (APC) Uninterruptible Power Supply (UPS) device for protection against the loss of power, a connection from the SmartSwitch device COM port to the UPS can be made to monitor the UPS power status. To use the COM port for this purpose, it must be reconfigured to support the UPS connection using the procedure described in Section 4.2.10. Refer to the UPS documentation for details on how to access the status information.

The Console Cable Kit provided with the SmartSwitch device is used to connect the UPS to the SmartSwitch device COM port as shown in Figure 2-2. To connect the UPS device to the COM port, proceed as follows:

1. Connect the RJ45 connector at one end of the cable to the COM port on the SmartSwitch device.
2. Plug the RJ45 connector at the other end of the cable into the RJ45-to-DB9 male (UPS) adapter (Enterasys Networks part number, 9372066).
3. Connect the RJ45-to-DB9 male (UPS) adapter to the female DB9 port on the rear of the UPS device (refer to the particular UPS device’s user instructions for more specific information about the monitoring connection).

Figure 2-2 Uninterruptible Power Supply (UPS) Connection



3

Accessing Local Management

This chapter provides information about the following:

- Navigating through the Local Management screen hierarchy for 802.1Q Switching (Section 3.1).
- Accessing the Password screen to enter a Local Management session (Section 3.2).
- Accessing the Device Menu screen and its menu items to gain access to the Local Management screens including the security screens (Section 3.3).
- Accessing the Security Menu screen to control access to the switch's host (Section 3.5).
- Accessing the Passwords (Section 3.6) and Radius Configuration (Section 3.7) screens. These screens allow you to configure additional security by limiting access to Local Management according to local access policy and remotely using the RADIUS Client feature.
- Accessing the Name Services Configuration screen (Section 3.8). This screen details additional security components to permit password authentication via a Radius Server.

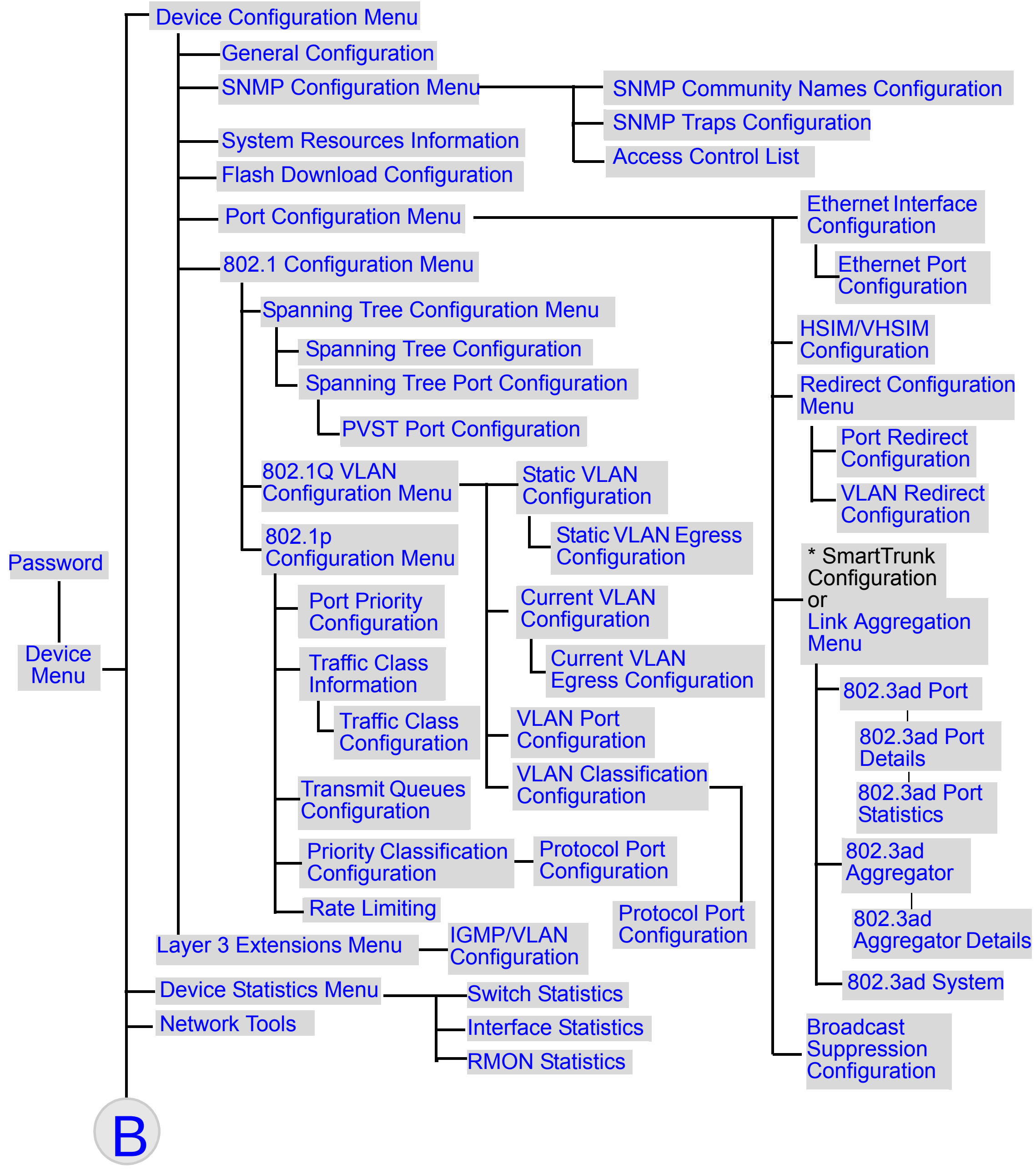
3.1 NAVIGATING LOCAL MANAGEMENT SCREENS

The switch Local Management application consists of a series of menu screens. Navigate through Local Management by selecting items from the menu screens.

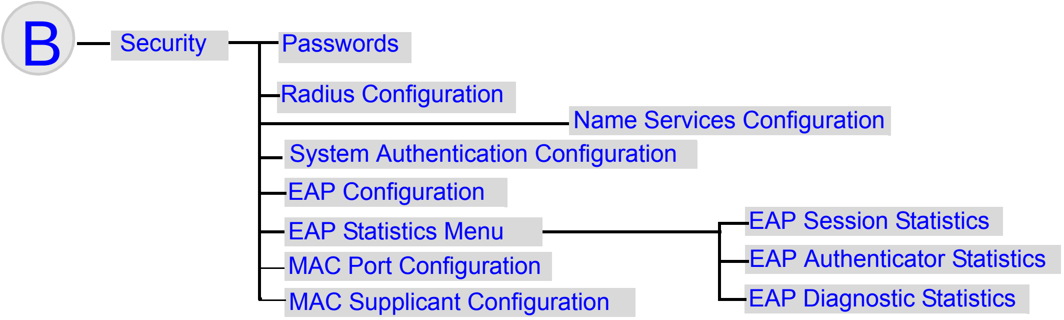
The hierarchy of the Local Management screens is shown in Figure 3-1.

NOTE: At the beginning of each chapter, a section entitled "Screen Navigation Path" shows the path to the first screen described in the chapter.

Figure 3-1 802.1Q Switching Mode, LM Screen Hierarchy


Device Configuration Menu
General Configuration
SNMP Configuration Menu
SNMP Community Names Configuration
SNMP Traps Configuration
Access Control List
System Resources Information
Flash Download Configuration
Port Configuration Menu
Ethernet Interface Configuration
Ethernet Port Configuration
802.1 Configuration Menu
Spanning Tree Configuration Menu
Spanning Tree Configuration
Spanning Tree Port Configuration
PVST Port Configuration
HSIM/VHSIM Configuration
Redirect Configuration Menu
Port Redirect Configuration
VLAN Redirect Configuration
802.1Q VLAN Configuration Menu
Static VLAN Configuration
Static VLAN Egress Configuration
802.1p Configuration Menu
* SmartTrunk Configuration or Link Aggregation Menu
Password
Device Menu
Port Priority Configuration
Current VLAN Configuration
Traffic Class Information
Current VLAN Egress Configuration
802.3ad Port
Traffic Class Configuration
VLAN Port Configuration
802.3ad Port Details
VLAN Classification Configuration
802.3ad Port Statistics
Transmit Queues Configuration
Priority Classification Configuration
Protocol Port Configuration
802.3ad Aggregator
Rate Limiting
Protocol Port Configuration
802.3ad Aggregator Details
Layer 3 Extensions Menu
IGMP/VLAN Configuration
802.3ad System
Device Statistics Menu
Switch Statistics
Network Tools
Interface Statistics
RMON Statistics
Broadcast Suppression Configuration
B

* Refer to the SmartTrunk User’s Guide for the screen hierarchy.


B
Security
Passwords
Radius Configuration
Name Services Configuration
System Authentication Configuration
EAP Configuration
EAP Statistics Menu
MAC Port Configuration
MAC Supplicant Configuration
EAP Session Statistics
EAP Authenticator Statistics
EAP Diagnostic Statistics

3.1.1 Selecting Local Management Menu Screen Items

Select items on a menu screen by performing the following steps:

1. Use the arrow keys to highlight a menu item.
2. Press ENTER. The selected menu item displays on the screen.

3.1.2 Exiting Local Management Screens

There are two ways to exit the Local Management (LM) screens.

Using the Exit Command

To exit LM using the EXIT screen command, proceed as follows:

1. Use the arrow keys to highlight the **EXIT** command at the bottom of the Local Management screen.
2. Press ENTER. The Local Management Password screen displays and the session ends.

Using the RETURN Command

To exit LM using the RETURN command, proceed as follows:

1. Use the arrow keys to highlight the **RETURN** command at the bottom of the Local Management screen.
2. Press ENTER. The previous screen in the Local Management hierarchy displays.

NOTE: The user can also exit Local Management screens by pressing ESC twice. This exit method does not warn about unsaved changes and all unsaved changes are lost.

3. Exit from Local Management by repeating steps 1 and 2 until the Device Menu screen displays.
4. To end the LM session, use the arrow keys to highlight the **RETURN** command at the bottom of the Device Menu screen.
5. Press ENTER. The Local Management Password screen displays and the session ends.

3.1.3 Using the NEXT and PREVIOUS Commands

If a particular Local Management screen has more than one screen to display its information, the NEXT and PREVIOUS commands are used to navigate between its screens.

To go to the next or previous display of a screen, proceed as follows:

1. Highlight the applicable **NEXT** or **PREVIOUS** command at the bottom of the screen.
2. Press ENTER. The screen displays.

3.1.4 Using the CLEAR COUNTERS Command

The CLEAR COUNTERS command is used to temporarily reset all counters of a screen to zero to allow you to observe counter activity over a period of time. To reset the counters, perform the following steps:

1. Use the arrow keys to highlight the **CLEAR COUNTERS** command.
2. Press ENTER, the counters are reset to zero.

3.2 PASSWORD SCREEN

When to Use

To access the Device Menu screen to start a Local Management session via a Telnet connection or local COM port connection. Whenever a connection is made to the switch, the Local Management Password screen displays. Before continuing, you must enter a password, which is compared to the previously stored passwords and associated management level access policy configured using the Security screen described in Section 3.5.

The level of management access is dependent on the password and the associated Access Policy configured in the Password Configuration screen described in Section 4.4.

NOTE: You can set the same string as a Security password and SNMP Community Name. This will allow you to access and manage the switch whether you are starting a Local Management session via a Telnet connection or local COM port connection, or by using a network SNMP management application.

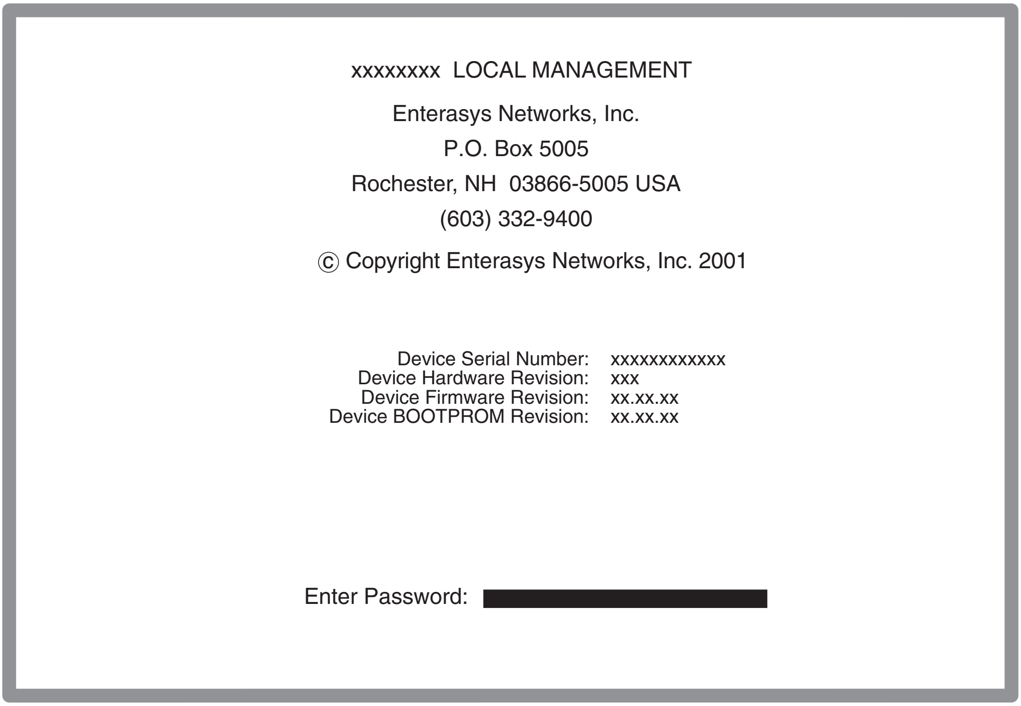
If you use a string for the security password and a different one for the SNMP Community Name, the two cannot be used interchangeably to access the switch. The access levels can also be configured to be different.

How to Access

Turn on the terminal. Press ENTER (this may take up to four times, because the COM port of the switch auto-senses the baud rate of the terminal) until the Local Management Password screen displays. Figure 3-2 shows the Password screen.

Screen Example

Figure 3-2 Local Management Password Screen



```
                    xxxxxxxx  LOCAL MANAGEMENT

                      Enterasys Networks, Inc.
                           P.O. Box 5005
                    Rochester, NH  03866-5005 USA
                          (603) 332-9400

                ⓒ Copyright Enterasys Networks, Inc. 2001


                   Device Serial Number:   xxxxxxxxxxxx
                Device Hardware Revision:  xxx
                Device Firmware Revision:  xx.xx.xx
              Device BOOTPROM Revision:    xx.xx.xx




              Enter Password:  
```

3650_10

Enter the Password and press ENTER. The default super-user access password is “*public*” or press ENTER.

NOTE: If an invalid password is entered, the terminal beeps and the cursor returns to the beginning of the password entry field.

Entering a valid password causes the associated access level to display at the bottom of the screen and the Device Menu screen to display.

If no activity occurs for a preset period of time, the Local Management Password screen redisplays and the password has to be reentered.

3.3 DEVICE MENU SCREEN

Screen Navigation Path

Password > **Device Menu**

When to Use

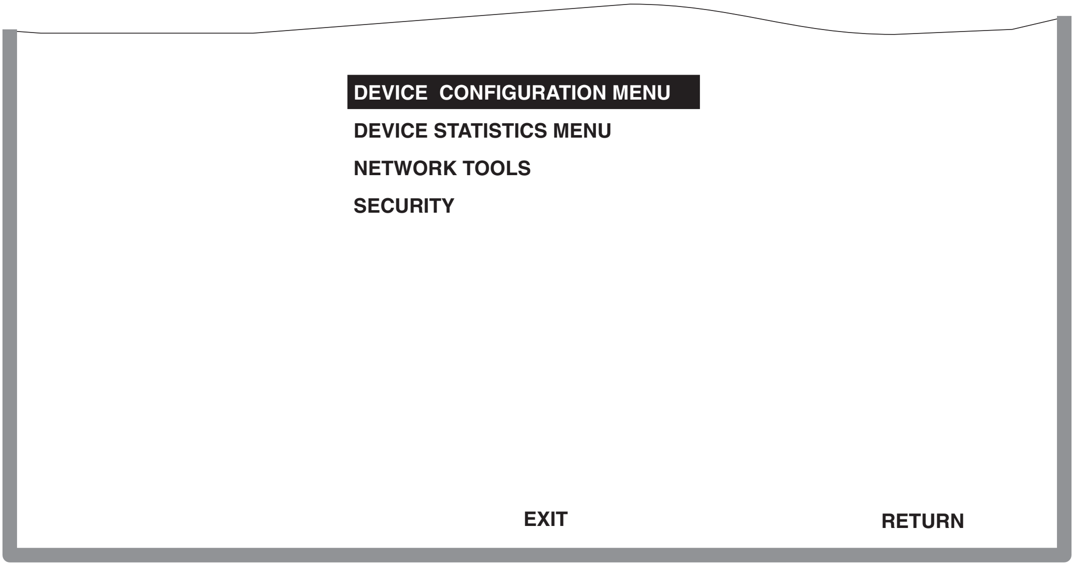
To access the Local Management screens of the switch.

How to Access

Enter a valid password in the Local Management Password screen as described in Section 3.2, and press ENTER. The Device Menu screen, Figure 3-3, displays.

Screen Example

Figure 3-3 Device Menu Screen



DEVICE CONFIGURATION MENU
DEVICE STATISTICS MENU
NETWORK TOOLS
SECURITY

EXIT
RETURN

35591_14

NOTE: If the terminal is idle for several minutes, the Local Management Password screen redisplays and the session ends. This idle time can be changed in the General Configuration screen described in Section 4.2.9.

Menu Descriptions

Refer to Table 3-1 for a functional description of each menu item.

Table 3-1 Device Menu Screen Menu Item Descriptions

Menu Item	Screen Function
DEVICE CONFIGURATION MENU	Provides access to the Local Management screens that are used to configure the switch and also provides access to the Port Configuration Menu screen, 802.1 Configuration Menu screens, and the Layer 3 Extensions Menu screens. The Port Configuration Menu screen provides access to the screens that are used to set operating parameters specific to each port. The 802.1 Configuration Menu screen provides access to the Spanning Tree Configuration Menu screen, 802.1Q VLAN Configuration Menu screen, and the 802.1p Configuration Menu screen. These screens are used to set the basic switch operations, and provide access to screens to configure VLANs, and assign port priorities. For details about the screens, refer to: Chapter 4 for the Device Configuration Menu screen, Chapter 5 for the Port Configuration Menu screen, Chapter 6 for the 802.1 Configuration Menu screen, and Chapter 9 for the Layer 3 Extensions Menu screen.
DEVICE STATISTICS MENU	Provides access to screens used to obtain statistics and performance information for the switch. For details, refer to Chapter 10.

Table 3-1 Device Menu Screen Menu Item Descriptions (Continued)

Menu Item	Screen Function
NETWORK TOOLS	The Network Tools function resides on the switch and consists of commands that allow the user to access and manage network devices, including the ability to Telnet to other devices. Chapter 11 explains how to use the Network Tools utility.
SECURITY	Provides access to the following screens: • Module Login Passwords • Radius Configuration • Name Services Configuration • System Authentication Configuration • EAP Configuration • EAP Statistics Menu • MAC Port Configuration • MAC Supplicant Configuration
	Provides access to the Password screen. This screen allows the user to set a login password for the device according to an access policy (read-only, read-write, and super-user). A different password can be set for each access policy. To prevent clearing the passwords, hardware switch 8 on the board of the device can be disabled using this screen. For an overview of the security available on this switch, refer to Section 3.4. For more information about the Module Login Password screen, refer to Section 3.6.

Table 3-1 Device Menu Screen Menu Item Descriptions (Continued)

Menu Item	Screen Function
SECURITY (cont'd)	The Radius Configuration screen enables you to configure the Radius client function on the switch to provide another restriction for access to the Local Management screens. For more information on Radius Client, refer to Section 3.4. For more information about the Radius Configuration screen, refer to Section 3.7.
	The System Authentication Configuration, EAP Configuration, and EAP Statistics Menu screens enable you to securely authenticate and grant appropriate access to end user devices directly attached to the switch ports. For more information about 802.1x port based network access control, refer to Section 3.4.2. For more information about the System Authentication Configuration, EAP Configuration, and EAP Statistics Menu screens, refer to Section 3.9, Section 3.10, and Section 3.11, respectively.
	The MAC Port Configuration screen enables you to monitor the authentication state of the supplicants associated with each port and enable/disable, initialize, and force a revalidation of the port MAC credential. For more information about MAC port configuration, refer to Section 3.12.
	The MAC Supplicant Configuration screen enables you to see which MAC authentication supplicants are active, their MAC address and associated module ports, and enable you to initialize or reauthenticate each of the supplicants. For more information about the MAC Supplicant Configuration screen, refer to Section 3.13.

3.4 OVERVIEW OF SECURITY METHODS

Six security methods are available to control which users are allowed access to the switch's host to monitor and control the switch.

- Login Security Password – used to access the Device Menu screen to start a Local Management session via a Telnet connection or local COM port connection. Whenever a connection is made to the switch, the Local Management Password screen displays. Before continuing, you must enter a login password, which is compared to the stored passwords and associated management level access policies configured using the Security screen described in Section 3.5.
- SNMP Community String – allows access to the switch via a network SNMP management application. To access the switch, you must enter an SNMP Community Name string. The level of management access is dependent on the SNMP Community Name and the associated Access Policy configured in the SNMP Community Names Configuration screen described in Section 4.4.

NOTES: You can set the same string as a Security login password and SNMP Community Name. This allows you to access and manage the switch whether you are starting a Local Management session via a Telnet connection or local COM port connection, or using a network SNMP management application.

If the login security password is different from the SNMP Community Name, the two cannot be used interchangeably to access the switch.

- Host Access Control Authentication (HACA) – authenticates user access of Telnet management, console local management and WebView via a central Radius Client/Server application using the Password screen described in Section 3.6. For an overview of HACA and a description of how to set the to access policy using the Radius Configuration screen, refer to Section 3.4.1 and Section 3.7.
- Host Access Control List (ACL) – allows only the defined list of IP Addresses to communicate with the host for Telnet, WebView (HTTP) and SNMP. To set up these parameters refer to the Host Access Control List (ACL) screen described in Section 4.6.
- 802.1X Port Based Network Access Control – provides a mechanism for administrators to securely authenticate and grant appropriate access to end user devices (supplicants) directly attached to switch ports. For more information, refer to Section 3.4.2.
- MAC Authentication – provides a mechanism for administrators to securely authenticate and grant appropriate access to end user devices directly attached to switch ports. For more information, refer to Section 3.4.3.

3.4.1 Host Access Control Authentication (HACA)

To use HACA, the embedded Radius Client on the switch must be configured to communicate with the Radius Server, and the Radius Server must be configured with the password information. The software used for this application provides the ability to centralize the Authentication, Authorization, and Accounting (AAA) of the network resources. For more information, refer to the RFC 2865 (Radius Authentication) and RFC 2866 (Radius Accounting) for a description of the protocol.

Each switch has its own Radius Client. The client can be configured via the Radius Configuration screen described in Section 3.7.

The **IP address** of the Radius Server and **shared secret text string** must be configured on the Radius Client. The client uses the Password Authentication Protocol (PAP) to communicate the user name and encrypted password to the Radius Server.

On the Radius Server, each user is configured with the following:

- name
- password
- access level

The access level can be set to one of the following levels for each user name:

- super-user
- read-write
- read-only

To support multiple access levels per user name, it involves sending back a different “FilterID” attribute using some server feature to differentiate between the same user name with different prefixes/suffixes. For example, “username@engineering” and “username@home” could each return different access levels.

NOTE: This is a server-dependent feature.

Only one password is allowed per access level. This enables the Radius Server to track the users accessing the switch host and how long they used the host application.

All radius values, except the server IPs and shared secrets, are assigned reasonable default values when radius is installed on a new switch. The defaults are as follows:

- Client, disabled
- Timeout, 20 seconds
- Retries, 3
- Primary and secondary Authentication ports: 1812 (per RFC 2865)
- Primary and secondary Accounting ports: 1813 (per RFC 2866)
- Last-resort for local and remote is CHALLENGE

If only one server is configured, it must be the primary server. It is not necessary to reboot after the client is reconfigured.

The client cannot be enabled unless the primary server is configured with at least the minimum configuration information.

NOTE: The minimum additional information that must be configured to use a server is its IP address and Shared Secret.

When the Radius Client is active on the switch, you are prompted by an authorization screen for a user login name and password when attempting to access the host IP address via the local console LM, Telnet to LM, or WebView application. The embedded Radius Client encrypts the information entered by the user and sends it to the Radius Server for validation. Then the server returns a yes or no response back to the client, allowing or denying the user to access the host application with the proper access level.

An access-accept response returns a message USER AUTHORIZATION = <ACCESS LEVEL> for 3 seconds and then the main screen of the application is displayed. An access-denied response causes an audible “beep” and the screen to return to the user name prompt.

If the Radius Client is unable to receive a response from the Radius Server, because the Radius Server is down or inaccessible, the Radius Client will time out to a default value of 20 seconds.

If the server returns an “access-accept” response (the user successfully authenticated), it must also return a Radius “FilterID” attribute containing an ASCII string with the following fields in the specified format:

“Enterasys:version=V:mgmt=M:policy=N”

Where:

V is the version number (currently V=1)

M is the access level for management, one of the following strings:

“su” for super-user access

“rw” for read-write access

“ro” for read-only access

N is the policy profile string (refer to the policy profile MIB)

NOTES:

1. Quotation marks (“ ”) are used for clarification only, and are not part of the command strings.
2. If the FilterID attribute is not returned, or the “mgmt” field is absent or contains an unrecognizable value, access to Local Management is denied.
3. Policy profiles are not yet deployed and the “policy=N” part may be omitted.

The secondary server is always consulted if it is configured. Note that the minimum additional information that must be configured to use a server is its IP and Shared Secret.

A backup secondary server is always consulted if it has been configured with its IP and Shared Secret. If communication is lost to all servers, and the user is connected to the local console serial port, the authorization screen will change to allow access to the switch by using the Local Management Module password.

If the user is connected remotely via TELNET or WebView, the switch will continue to deny access until communication with the Radius Server is operational again. Optionally, if the switch has been configured to allow remote access, the switch can be configured to use the Local Management Module password in the event of a Radius failure.

3.4.2 802.1X Port Based Network Access Control

This section provides

- a brief description of 802.1X Port Based Network Access Control,
- definitions of common terms and abbreviations, and
- an overview of the tasks that may be accomplished using the 802.1X and EAP security and authentication features.

When using the physical access characteristics of IEEE 802 LAN infrastructures, the 802.1X standard provides a mechanism for administrators to securely authenticate and grant appropriate access to end user devices directly attached to switch ports. When configured in conjunction with NetSight Policy Manager and Radius server(s), Enterasys Networks' switchs can dynamically administer user based policy that is specifically tailored to the end user's needs.

3.4.2.1 Definitions of Terms and Abbreviations

Table 3-2 provides an explanation of authentication terms and abbreviations used when describing the 802.1X and EAP security and authentication features.

Table 3-2 Authentication Terms and Abbreviations

Term	Definition
EAP	Extensible Authentication Protocol (e.g., Microsoft IAS Server and Funk Steel Belted Radius).
PAE	Port Access Entity, device firmware that implements or participates in the protocol.
PWA	Port Web Authentication, an enterprise specific authentication process using a web browser user-login process to gain access to ports.
RADIUS	Remote Authentication Dial In User Service.
Authenticator	The entity that sits between a supplicant and the authentication server. The authenticator's job is to pass authenticating information between the supplicant and authentication server until an authentication decision is made.

Table 3-2 Authentication Terms and Abbreviations (Continued)

Term	Definition
Authentication Server	Provides authentication service to an authenticator. This service determines, by the credentials the supplicant provides, whether a supplicant is authorized to access services provided by the authenticator. The authentication server can be co-located with an authenticator or can be accessed remotely.
Supplicant	The entity (user machine) that is trying to be authenticated by an authenticator attached to the other end of that link.

3.4.2.2 802.1X Security Overview

The Enterasys Networks' SmartSwitch 2200 Series modules support the following 802.1X and EAP security and authentication features to:

- Authenticate hosts that are connected to dedicated switch ports.
- Authenticate based on single-user hosts. (If a host is a time-shared Unix or VMS system, successful authentication by any user will allow all users access to the network.)
- Allow users to authenticate themselves by logging in with user names and passwords, token cards, or other high-level identification. Thus, a system manager does not need to spend hours setting low-level MAC address filters on every edge switch to simulate user-level access controls.
- Divide system functionality between supplicants (user machines), authenticators, and authentication servers. Authenticators reside in edge switches. They shuffle messages and tell the switch when to grant or deny access, but do not validate logins. User validation is the job of authentication servers. This separation of functions allows network managers to put authentication servers on central servers.
- Use the 802.1X protocol to communicate between the authenticator and the supplicant. the frame format using 802.1X incl;udes extra data fields within a LAN frame. Note that 802.1X does not allowrouting.
- Use the 802.1X protocol to communicate between the authenticator and the authentication server. The specific protocol that runs between these components (e.g., RADIUS-encapsulated EAP) is not specified and is implementation-dependent.

3.4.3 MAC Authentication Overview

This section discusses a method for a user to gain access to the network by validating the MAC address of their connected device. Network management statically provisions MAC addresses in a central radius server. Those pre-configured MAC addresses are allowed access to the network through the usual RADIUS validation process. This section further discusses how MAC Authentication and 802.1X cooperate to provide an integrated approach to authentication.

3.4.3.1 Authentication Method Selection

The 802.1X and PWA authentication methods are globally exclusive. Additionally, MAC Authentication and PWA are globally mutually exclusive. However, MAC Authentication and 802.1X are not mutually exclusive, so that both 802.1X and MAC authentications can be configured concurrently on the same device using the Local Management (LM) System Authentication Configuration screen described in Section 3.9. When both methods are enabled on the same device, the switch enforces a precedence relationship between MAC Authentication and 802.1X methods.

When configuring a device using the System Authentication Configuration screen, only the valid set of global and per port authentication methods are available for selection. These are EAP, PWA, MAC, MAC EAP, and NONE. If there is an attempt to enable both MAC Authentication and PWA either through the sole use of MIBs or by using both the LM screen and MIBs, then an appropriate error message is displayed.

3.4.3.2 Authentication Method Sequence

When MAC Authentication is enabled on a port, the Authentication of a specific MAC address commences immediately following the reception of any frame. The MAC address and a currently stored password for the port are used to perform a PAP authentication with one of the configured radius servers. If successful, the port forwarding behavior is changed according to the authorized policy and a session is started. If unsuccessful, the forwarding behavior of the port remains unchanged.

If successful, the filter-id in the radius response may contain a policy string of the form policy=”policy name”. If the string exists and it refers to a currently configured policy in this switch, then the port receives this new policy. If authenticated, but the authorized policy is invalid or non-existent, then the port forwards the frame normally according to the port default policy, if one exists. Otherwise, frames are forwarded without any policy.

3.4.3.3 Concurrent Operation of 802.1X and MAC

Authentication

This section defines the precedence rules to determine which authentication method, 802.1X (EAP) or MAC Authentication has control over an interface. Setting the 802.1X and MAC port authentication is described in Section 3.9.

When both methods are enabled, 802.1X takes precedence over MAC Authentication when a user is authenticated using the 802.1X method. If the port or MAC remains unauthenticated in 802.1X, then MAC authentication is active and may authenticate the next MAC address received on that port.

It is also recommended to have a state whereby 802.1X is completely disabled on a port leaving MAC-Authentication active. 802.1X does not explicitly provide any per port enable or disable of its authentication mechanism.

You can configure MAC Authentication and 802.1X to run concurrently on the same module, but exclusively on distinct interfaces of that module. To achieve this, the 802.1X port behavior in the force-unauthorized state is overloaded. When 802.1X and MAC Authentication are enabled, setting the 802.1X MIB to force-unauthorized for the interface in question and enabling MAC Authentication. This allows the MAC Authentication to run unhindered by 802.1X on that interface. This, in effect, disables all 802.1X control over that interface. However, if a default policy exists on that port, the switch forwards the frames according to that policy, otherwise the switch drops them.

If a switch port is configured to enable both 802.1X and MAC Authentication, then it is possible for the switch to receive a start or a response 802.1X frame while a MAC Authentication is in progress. If this situation, the switch immediately aborts MAC Authentication. The 802.1X authentication then proceeds to completion. After the 802.1X login completes, the user has either succeeded and gained entry to the network, or failed and is denied access to the network. Regardless of success, after the 802.1X login attempt, no new MAC Authentication logins occur on this port until:

- A link is toggled.
- The user executes an 802.1X logout.
- Management terminates the 802.1X session.

NOTE: The switch may terminate a session in many different ways. All of these reactivate the MAC authentication method. Refer to Table 3-3 for the precedence relationship between MAC and 802.1X authentication.

When a port is set for concurrent use of MAC and 802.1X authentication, the switch continues to issue EAPOL request/id frames until a MAC Authentication succeeds or the switch receives an EAPOL response/id frame.

Table 3-3 MAC / 802.1X Precedence States

802.1X Port Control	MAC Port Control	Authenticated?	Default Policy Exists?	Authorized Policy Exists?	Action
Force Authorized	Don't Care	Don't Care	Yes	Don't Care	• Neither method performs authentication. • Frames are forwarded according to default policy.
Force Authorized	Don't Care	Don't Care	No	Don't Care	• Neither method performs authentication. • Frames are forwarded.
Auto	Enabled	Yes	Don't Care	Yes	• Hybrid authentication (both methods are active). • Frames are forwarded according to authorized policy.
Auto	Enabled	Yes	Yes	No	• Hybrid authentication (both methods are active). • Frames are forwarded according to default policy.
Auto	Enabled	Yes	No	No	• Hybrid authentication (both methods active). • Frames are forwarded.
Auto	Enabled	No	Yes	Don't Care	• Hybrid authentication (both methods are active). • Frames are forwarded according to default policy.
Auto	Enabled	No	No	Don't Care	• Hybrid authentication (both methods are active). • Frames are discarded.

Table 3-3 MAC / 802.1X Precedence States (Continued)

802.1X Port Control	MAC Port Control	Authen-ticated?	Default Policy Exists?	Autho-rized Policy Exists?	Action
Auto	Disabled	Yes	Don’t Care	Yes	• 802.1X performs authentication. • Frames are forwarded according to authorized policy.
Auto	Disabled	Yes	Yes	No	• 802.1X performs authentication. • Frames are forwarded according to default policy.
Auto	Disabled	Yes	No	No	• 802.1X performs authentication. • Frames are forwarded.
Auto	Disabled	No	Yes	Don’t Care	• 802.1X performs authentication. • Frames are forwarded according to default policy.
Auto	Disabled	No	No	Don’t Care	• 802.1X performs authentication. • Frames are discarded.
Force Unauthorization	Enabled	Yes	Don’t Care	Yes	• MAC performs authentication. • Frames are forwarded according to authorized policy.
Force Unauthorization	Enabled	Yes	Yes	No	• MAC performs authentication. • Frames are forwarded according to default policy.
Force Unauthorization	Enabled	Yes	No	No	• MAC performs authentication. • Frames are forwarded.
Force Unauthorization	Enabled	No	Yes	Don’t Care	• MAC performs authentication. • Frames are forwarded according to default policy.

Table 3-3 MAC / 802.1X Precedence States (Continued)

802.1X Port Control	MAC Port Control	Authen-ticated?	Default Policy Exists?	Autho-rized Policy Exists?	Action
Force Unauthorization	Enabled	No	No	Don't Care	• MAC performs authentication. • Frames are discarded.
Force Unauthorization	Disabled	Don't Care	Don't Care	Don't Care	• Neither method performs authentication. • Frames are discarded.

3.4.4 MAC Authentication Control

This global variable can be set to enabled or disabled.

If set to enabled, then

a. MAC Authentication is active on those ports whose individual port-enabled variable is set to enabled.

b. All session and statistic information is reset to defaults.

c. Any MAC addresses currently locked to ports are unlocked.

If set to disabled, then

a. MAC Authentication stops for all ports.

b. All active sessions are terminated with the cause portAdminDisabled.

c. All policies are applied to ports as a result of a MAC Authentication reverting to the ports default policy, if any.

d. All ports currently authenticated using 802.1X, are unaffected.

e. Any 802.1X ports, which were set to forced-unauth, revert back to discarding all frames regardless of the MAC Authentication state.

3.5 SECURITY MENU SCREEN

Screen Navigation Path

Password > Device Menu > **Security**

When to Use

To access the Passwords, Radius Configuration, Name Services Configuration, System Authentication Configuration, EAP Configuration, EAP Statistics Menu, MAC Port Configuration, and MAC Supplicant Configuration screens.

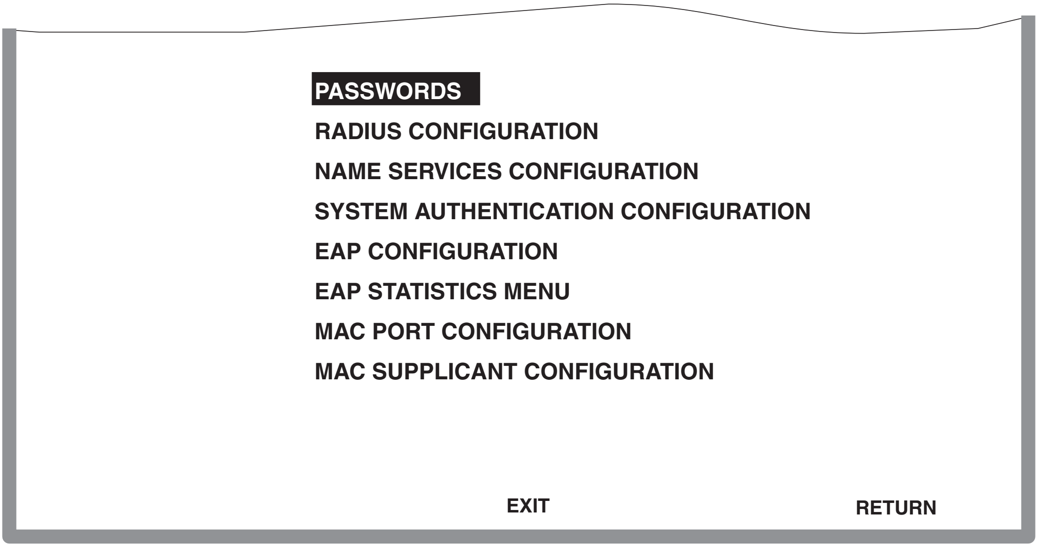
- The Passwords and Radius Configuration screens allow you to configure additional limited access.
- The Name Services Configuration screen allows you to set parameters for personalized web authentication.
- The System Authentication Configuration, EAP Configuration, EAP Statistics Menu screens enable you to view port authentication type and status, to configure EAP settings, and to view EAP statistics.
- The MAC Port Configuration and MAC Supplicant Configuration screens enable you to configure MAC Authentication for user devices (supplicants) directly attached to one or more physical ports.

How to Access

Use the arrow keys to highlight the **SECURITY** menu item on the Device Configuration Menu screen and press ENTER. The Security Menu screen, Figure 3-4, displays.

Screen Example

Figure 3-4 Security Menu Screen



3528_14

Menu Descriptions

Refer to Table 3-4 for a functional description of each menu item.

Table 3-4 Security Menu Screen Menu Item Descriptions

Menu Item	Screen Function
PASSWORDS	Used to set the Locally Administered Passwords (super user, read-write, and read-only) to access the device according to an access policy. For details, refer to Section 3.6.
RADIUS CONFIGURATION	Used to configure the Radius Client Parameters on the switch, primary server, and secondary server. For details, refer to Section 3.7.
NAME SERVICES CONFIGURATION	Used to set parameters for personalized Web authentication, including the URL and IP of the Secure Harbour web page. For details, refer to Section 3.8.
SYSTEM AUTHENTICATION CONFIGURATION	Used to enable or disable an authentication type for the device, and to display the authentication type and authentication status (enabled or disabled) for all ports. For details, refer to Section 3.9.
EAP CONFIGURATION	Used to configure authentication settings for each port. For details, refer to Section 3.10.
EAP STATISTICS MENU	Used to navigate to the EAP Session Statistics, EAP Authentication Statistics, and EAP Diagnostic Statistics screens. For details, refer to Section 3.11.
MAC PORT CONFIGURATION	Used to view the current port authentication states, enable or disable the authentication function on each port, reset ports to the initial authentication configuration, and force a revalidation of the MAC credential. For details, refer to Section 3.12.
MAC SUPPLICANT CONFIGURATION	Used to show how long MAC Authentication supplicants are logged on to a port and their MAC address, and provides limited configuration of these supplicants. For details, refer to Section 3.13.

3.6 PASSWORDS SCREEN

When to Use

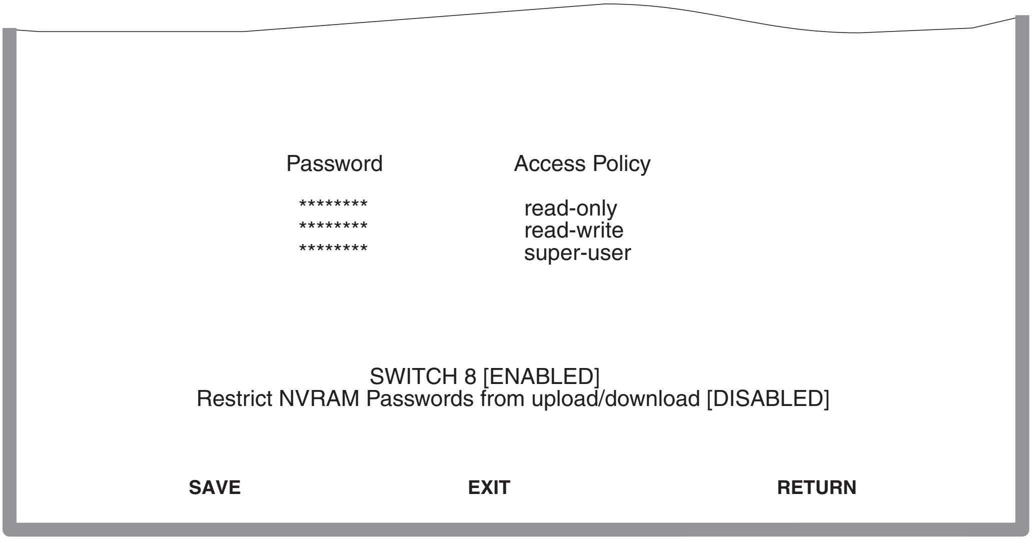
To provide additional security by using login passwords associated to an access policy. This screen allows the use of passwords to provide three levels of Local Management access (super-user, read-write and read-only) via serial console or telnet connection. This screen is also used to disable the function of hardware switch 8 to prevent the clearing of the login passwords.

How to Access

Use the arrow keys to highlight the **PASSWORDS** menu item on the Security Menu screen and press ENTER. The Module Login Passwords screen, Figure 3-5, displays.

Screen Example

Figure 3-5 Module Login Passwords Screen



```
Password          Access Policy

********           read-only
********           read-write
********           super-user


               SWITCH 8 [ENABLED]
Restrict NVRAM Passwords from upload/download [DISABLED]
```

Field Descriptions

Refer to Table 3-5 for a functional description of each screen field.

Table 3-5 Module Login Passwords Screen Field Descriptions

Use this field…	To…	
Password (Modifiable)	Enter the password used to access the device according to an access policy.	
Access Policy (Read-only)	See the access given each password. Possible selections are as follows:	
	read-only	This password allows read-only access to the Local Management, and excludes access to security-protected fields of read-write or super-user authorization.
	read-write	This password allows read and write access to Local Management, excluding security protected fields for super-user access only.
	super-user	This password permits read-write access to Local Management and allows the user to change all modifiable parameters including community names, IP addresses, traps, and SNMP objects.
SWITCH 8 (Toggle)	Enable or disable the function of hardware switch S8 on the main board of the device. When set to ENABLED, S8 can be used to clear the password. When set to DISABLED, S8 cannot be used to clear the password. The default is Enable.	
Restrict NVRAM Passwords from Upload/Download (Toggle)	Prevent passwords residing in NVRAM from being replaced when downloading a configuration file. The default setting is DISABLED. This prevents the passwords from being downloaded.	

3.6.1 Setting the Module Login Password

Setting the Module Login Password provides additional security by assigning each switch its own password and allows you to disable the function of switch S8 so that the password cannot be cleared.

To assign the password and disable switch S8, proceed as follows:

1. Use the arrow keys to highlight the appropriate **Password** field. A different password can be assigned to each Access Policy.
2. Press ENTER.
3. To disable the function of switch S8 so the passwords cannot be cleared, use the arrow keys to highlight the **Switch 8** field.
4. Press the SPACE bar to select **DISABLED**.
5. To save the settings, press ENTER. The message “SAVED OK” displays at the top of the screen.

3.7 RADIUS CONFIGURATION SCREEN

When to Use

To configure the Radius client in the switch to restrict access to the management functions of the Local Management screens, by way of the COM port or network TELNET connection.

NOTE: The configuration and Enable State of the Radius client will be stored in NVRAM and loaded on power-up. If the client is properly configured and enabled, the platform will create the Radius client and enable it at boot time, superseding legacy authentication. Otherwise, the legacy authentication becomes operational.

Radius Client parameters can also be set using the Network Tools screen described in Chapter 11.

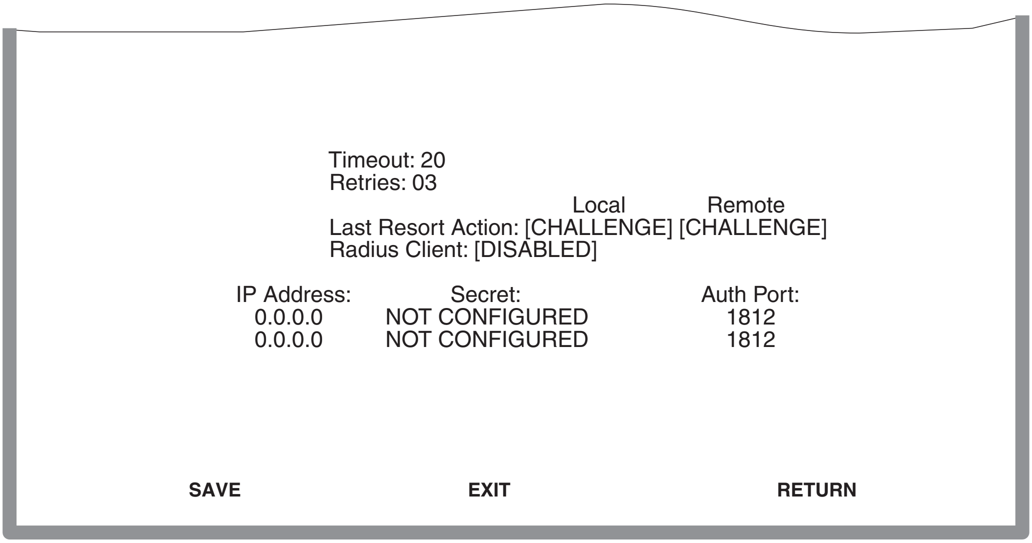
This screen allows you to set the necessary parameters to centralize the Authentication, Authorization, and Accounting of the network resources. For information about Radius Client and how it functions, refer to Section 3.4 and Section 3.4.1.

How to Access

Use the arrow keys to highlight the **RADIUS CONFIGURATION** menu item on the Security Menu screen and press ENTER. The Radius Configuration screen, Figure 3-6, displays.

Screen Example

Figure 3-6 Radius Configuration Screen



```
                        Timeout: 20
                        Retries: 03
                                               Local          Remote
                        Last Resort Action: [CHALLENGE] [CHALLENGE]
                        Radius Client: [DISABLED]

                IP Address:            Secret:                  Auth Port:
                  0.0.0.0         NOT CONFIGURED                  1812
                  0.0.0.0         NOT CONFIGURED                  1812
```

Field Descriptions

Refer to Table 3-6 for a functional description of each screen field.

Table 3-6 Radius Configuration Screen Field Descriptions

Use this field…	To…
Timeout (Modifiable)	Enter the maximum time in seconds to establish contact with the Radius Server before timing out. The default is 20 seconds.
Retries (Modifiable)	Enter the maximum number of attempts (1…N) to contact the Radius Server before timing out. The default is 20 seconds.

Table 3-6 Radius Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Last Resort Action/Local (Selectable)	Accept, Challenge, and Reject, which do the following: ACCEPT: Allows local access (via COM port) at the super-user level with no further attempt at authentication. CHALLENGE: Reverts to local module (legacy) passwords. REJECT: Does not allow local access. For more details, refer to Section 3.7.1. To set local and remote servers, refer to Section 3.7.2.
Last Resort Action/Remote (Toggle)	Accept, Challenge, and Reject, which do the following: ACCEPT: Allows remote access (via Telnet or WebView) at the super-user level with no further attempt at authentication. CHALLENGE: Reverts to local module (legacy) passwords. REJECT: Does not allow remote access. For more details, refer to Section 3.7.1. To set local and remote servers, refer to Section 3.7.2.
Radius Client (Toggle)	Enable or disable client status.
IP Address (Modifiable)	Enter the IP address (in decimal-dot format) of the primary and secondary servers being configured for the RADIUS function.
Secret (Modifiable)	Enter a secret string of characters or the primary and secondary server (16 characters are recommended as per RFC 2865). The maximum is 32 characters).
Auth Port (Modifiable)	Enter the number of the Authorization UDP Port for the Primary and Secondary server.

3.7.1 Setting the Last Resort Authentication

The Radius client can be configured to use primary and secondary servers. If the primary server does not respond within the specified number of retries during the specified time-out period, the client will then attempt to authenticate using the secondary server. If the secondary server also does not respond, then the client returns a time-out condition.

The "last resort" platform action in case of Radius server time-out for both local and remote access is selectable for each type of access:

- Local login via the COM port.
- Remote login via a remote network TELNET connection.

3.7.2 Setting the Local and Remote Servers

Before setting the parameters, refer to Section 3.4.1 and Section 3.7.1 for a better understanding of Radius Servers and Last Resort Authentication. To set the local and remote server, proceed as follows:

1. Highlight the **Timeout** field and enter the maximum time in seconds to establish contact with the Radius Server before timing out.
2. Highlight the **Retries** field and enter the desired maximum number of attempts (1…N) to contact the Radius Server before timing out.
3. Highlight the **Last-Resort Action/Local** field and select **ACCEPT**, **CHALLENGE**, or **REJECT** to allow local access at the super-user level with no further attempt at authentication; revert local module to (legacy) passwords, or not allow local access.
4. Highlight the **Last-Resort Action/Remote** field select **ACCEPT**, **CHALLENGE**, or **REJECT** to allow remote access at the super-user level with no further attempt at authentication, revert remote module to (legacy) passwords, or not allow remote access, respectively.
5. Use the arrow keys to highlight the **IP Address** field and enter the IP address (in decimal-dot format) of the primary and secondary servers being configured for the RADIUS function.
6. Highlight the **Secret** field and enter a secret string of characters or the primary and secondary server (16 characters are recommended as per RFC 2865. The maximum is 32 characters).
7. Highlight the **Auth Port** field and enter the number of the Accounting UDP Port for the Primary and Secondary server.
8. Use the arrow keys to highlight the **SAVE** command and press ENTER to save your settings.

3.8 NAME SERVICES CONFIGURATION SCREEN

When to Use

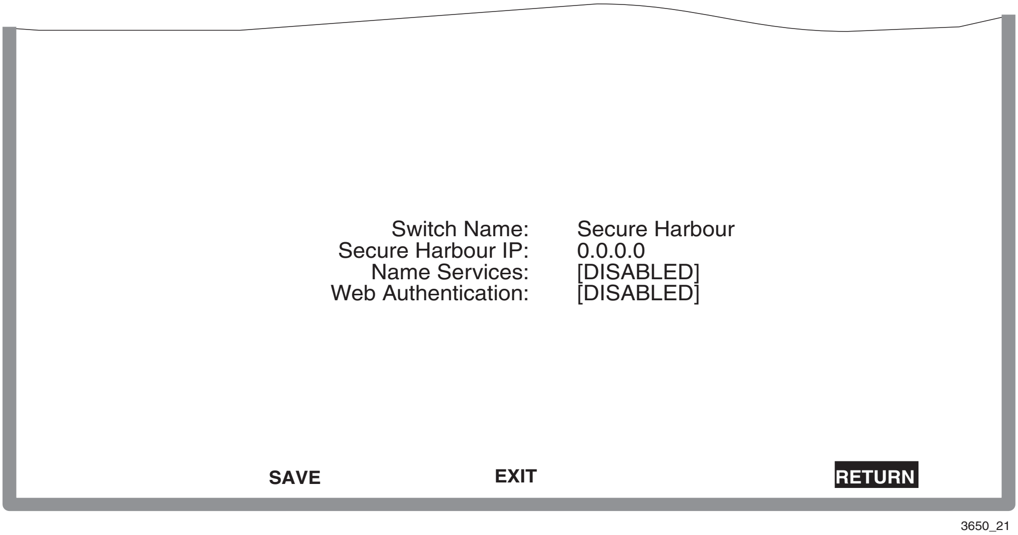
Use this screen when enabling Port-based Web authentication. This screen can also be used to configure the global Secure Harbour name and IP address. The user can Enable/Disable Name Services and associate the switch name with the Secure Harbour IP address.

How to Access

Use the arrow keys to highlight the **NAME SERVICES CONFIGURATION** menu item on the Security Menu screen and press ENTER. The Name Services Configuration screen, Figure 3-7, displays.

Screen Example

Figure 3-7 Name Services Configuration Screen



```
        Switch Name:      Secure Harbour
  Secure Harbour IP:      0.0.0.0
      Name Services:      [DISABLED]
 Web Authentication:      [DISABLED]
```

Field Descriptions

Refer to Table 3-7 for a functional description of each screen field.

Table 3-7 Name Services Configuration Screen Field Descriptions

Use this field…	To…
Switch Name (Modifiable)	Create a textual name to bind to the IP address. **NOTE:** The switch Name and the Secure Harbour IP must be globally unique within your network and the end switch must contain the identical information.
Secure Harbour IP (Read-Only)	See the IP address used to access services. **NOTE:** The Switch Name and the Secure Harbour IP must be globally unique within your network and the end switch must contain the identical information. The Secure Harbour IP cannot be the same as the management IP of the switch.
Name Services (Toggle)	Enable or disable the name services function.
Web Authentication (Toggle)	Enable or disable Web Authentication.

3.9 SYSTEM AUTHENTICATION CONFIGURATION SCREEN

When to Use

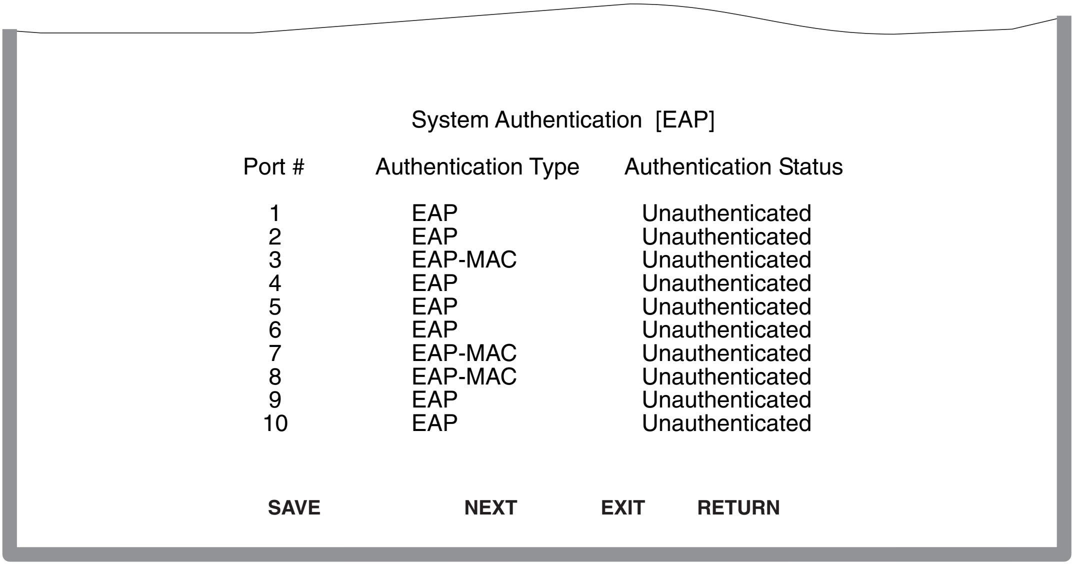
To enable or disable an authentication type for the device, and to display the authentication type and authentication status (enabled or disabled) for all ports.

How to Access

Use the arrow keys to highlight the **SYSTEM AUTHENTICATION CONFIGURATION** menu item on the Security Menu screen and press ENTER. The System Authentication Configuration screen, Figure 3-8, displays.

Screen Example

Figure 3-8 System Authentication Configuration Screen



```
                    System Authentication  [EAP]

   Port #        Authentication Type      Authentication Status

     1               EAP                     Unauthenticated
     2               EAP                     Unauthenticated
     3               EAP-MAC                 Unauthenticated
     4               EAP                     Unauthenticated
     5               EAP                     Unauthenticated
     6               EAP                     Unauthenticated
     7               EAP-MAC                 Unauthenticated
     8               EAP-MAC                 Unauthenticated
     9               EAP                     Unauthenticated
    10               EAP                     Unauthenticated
```

37831-02

Field Descriptions

Refer to Table 3-8 for a functional description of each screen field.

Table 3-8 System Authentication Configuration Screen Field Descriptions

Use this field…	To…
System Authentication (Selectable)	Enable or disable an authentication type for the device, or turn off the port authentication function on all ports. Options are **EAP** (Extensible Authentication Protocol), **PWA** (Port Web Authentication), **MAC** (Machine Address Code), **EAP MAC**, or **NONE**. • EAP is encapsulated in LAN frames according to the 802.1X standard. • PWA uses the web browser user login process to allow access to ports. • MAC authentication limits access to the network by validating the MAC address of their connected devices. • EAP MAC enables using both MAC and EAP authentication methods concurrently for security. • **NONE** turns off all port authentication in the switch. The default is NONE. To select the option, use the arrow keys to highlight the **System Authentication** field, step to **EAP**, **PWA**, **MAC**, **EAP MAC**, or **NONE** using the SPACE bar, then press ENTER.
Port # (Read-Only)	See the port numbers of all ports known to the device. Up to 10 ports can be displayed at a time. To see additional ports, select NEXT and press ENTER to display the authentication type and status for the next 10 ports.
Authentication Type (Read-Only)	See the authentication type configured for each port: **EAP**, **PWA**, **MAC**, **EAP MAC**, or **NONE**.
Authentication Status (Read-Only)	See whether the port is authenticated for the chosen authentication type. Status is **Authenticated**, **EAP Authenticated**, **MAC Authenticated**, or **Unauthenticated**.

3.10 EAP (PORT) CONFIGURATION SCREEN

When to Use

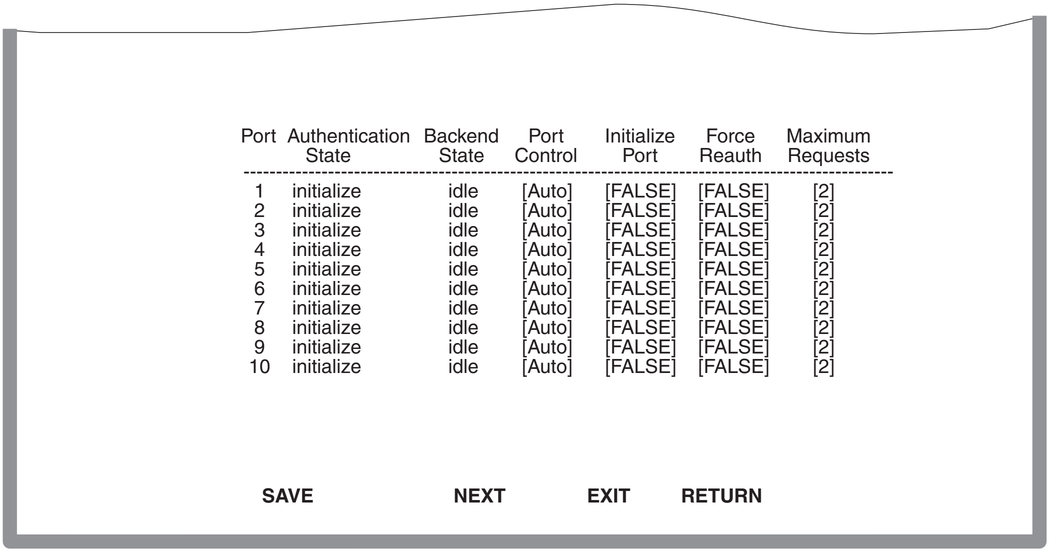
To configure authentication settings for each port.

How to Access

Use the arrow keys to highlight the **EAP CONFIGURATION** menu item on the Security Menu screen and press ENTER. The EAP Port Configuration screen, Figure 3-9, displays.

Screen Example

Figure 3-9 EAP Port Configuration Screen



```
Port Authentication  Backend   Port     Initialize   Force     Maximum
          State        State   Control     Port      Reauth    Requests
----------------------------------------------------------------------
  1   initialize       idle    [Auto]    [FALSE]    [FALSE]      [2]
  2   initialize       idle    [Auto]    [FALSE]    [FALSE]      [2]
  3   initialize       idle    [Auto]    [FALSE]    [FALSE]      [2]
  4   initialize       idle    [Auto]    [FALSE]    [FALSE]      [2]
  5   initialize       idle    [Auto]    [FALSE]    [FALSE]      [2]
  6   initialize       idle    [Auto]    [FALSE]    [FALSE]      [2]
  7   initialize       idle    [Auto]    [FALSE]    [FALSE]      [2]
  8   initialize       idle    [Auto]    [FALSE]    [FALSE]      [2]
  9   initialize       idle    [Auto]    [FALSE]    [FALSE]      [2]
 10   initialize       idle    [Auto]    [FALSE]    [FALSE]      [2]
```

Field Descriptions

Refer to Table 3-9 for a functional description of each screen field.

Table 3-9 EAP Port Configuration Screen Field Descriptions

Use this field…	To…
Port (Read-Only)	See the port number of all ports known to the device. Up to 10 ports can be displayed as a time. Highlight NEXT and press ENTER to display the next set of ports.
Authentication State (Read-Only)	See the current authentication state of each port. These following nine described states are the possible internal states for the authenticator. Some states are simply pass-through states causing a small action and immediately moving to a new state. Therefore, not all states can be observed for this interface.
	• **initialize**: A port is in the initialize state when: **a.** EAP authentication is disabled, **b.** EAP authentication is enabled and the port is not linked, or **c.** EAP authentication is enabled and the port is linked. (In this case very little time is spent in this state, it immediately transitions to the connecting state, via disconnected.
	• **disconnected**: The port passes through this state on its way to connected whenever the port is reinitialized, via link state change, reauthentication failure, or management intervention.
	• **connecting**: While in this state, the authenticator sends request/ID messages to the supplicant.
	• **authenticating**: The port enters this state from connecting after receiving a response/ID from the supplicant. It remains in this state until the entire authentication exchange between the supplicant and the authentication server completes.
	• **authenticated**: The port enters this state from authenticating state after the exchange completes with a favorable result. It remains in this state until linkdown, logoff, or until a reauthentication begins.

Table 3-9 EAP Port Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Authentication State (Cont'd)	• **aborting**: The port enters this state from authenticating when any event occurs that interrupts the login exchange.
	• **held**: After any login failure, this state is entered where the port remains for the number of seconds equal to quietPeriod (can be set using mib).
	• **forceAuth**: Management has set this in "Port Control". This allows normal, unsecured switching on this port.
	• **forceUnauth**: Management has set this in "Port Control". Absolutely no frames are forwarded to or from this port.
Backend State (Read-Only)	See the current backend state of each port. The backend state machine controls the protocol interaction between the authenticator (the switch) and the authentication server (typically a radius server). These following seven states are the possible internal states for the authenticator. Some states are simply pass-through states causing a small action and immediately moving to a new state. Therefore, you may not observe all of the states in this interface. For more detail, please see the IEEE Standard 802.1X-20001, Port Based Network Access Control.
	• **request**: The port has received a request from the server and is waiting for a response from the supplicant.
	• **response**: The port has received a response from the server and is waiting for either another request or an accept or reject from the server.
	• **success**: The port has received a success from the server. Send a success to the supplicant and move to idle.
	• **fail**: The port has received a reject from the server. Send a fail to the supplicant and move to idle.
	• **timeout**: The port has timed-out during the authentication exchange.

Table 3-9 EAP Port Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Backend State (Cont'd)	• **idle**: The port is currently not involved in any authentication, but is ready to begin one. Move to idle after completion.
	• **initialize**: The port is initializing the relevant backend variables and is not ready to begin an authentication. Move to idle after completion.
Port Control (Selectable)	Set the port control mode enabling network access for each port. Modes include: • **Auto**: In this mode, frames are forwarded according to the authentication state of each port. When no default policy has been applied to the port, and its authentication state is unauthorized, the port discards all incoming and outgoing frames. If a default policy is applied to the port and its authentication state is unauthorized, frames are forwarded according to the configuration specified for that policy. Once authorized, a port forwards frames according to its current configuration. A policy string may be returned by the Radius Server in the filter id attribute. This policy string can reference a set of VLAN and priority classification rules pre-configured in the switch. If a policy string is returned as part of the user authorization process, then frames are forwarded according to the configuration specified by that policy. If no policy is returned, the switch forwards frames using the existing default policy configuration, if it exists, or the current configuration for the port if no default policy exists. If the default policy is used, then we interpret that default policy to now be active on the controlled port. Although continuing to use the default policy after authorization may be a legal configuration, there are no practical uses. If a policy string is returned that has no definition in the switch, then this is an illegal configuration and the port is not authenticated. Therefore frame forwarding in this case follows the rules outlined above for an unauthorized port.

Table 3-9 EAP Port Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Port Control (Cont'd)	• **Forced Authenticated Mode**: The Forced Authenticated Mode is meant to disable authentication on a port. It is intended for ports that support ISLs and devices that cannot authenticate, such as printers and file servers. If a default policy is applied to the port via the Policy Profile MIB, then frames are forwarded according to the configuration set by that policy, otherwise frames are forwarded according to the current configuration for that port. Authentication using 802.1X is not possible on a port in this mode.
	• **Forced Unauthenticated Mode**: When a port is set to the Forced Unauthenticated Mode, all frames received on the port are discarded by a filter. Authentication using 802.1X is not possible on a port in this mode.
Initialize Port (Single Setting)	Set to **TRUE** to initialize all state machines for this port. After initialization, authentication can proceed normally on this port according to its control settings. This has the effect of kicking off any currently authorized user on the port and resetting the session information for a new login. You can only set this field to TRUE to initialize the port. Afterwards the field immediately reverts to FALSE.
Force Reauth (Single Setting)	Set to **TRUE** to cause an immediate forced reauthentication for a user who is currently logged on to the port. If the reauthentication fails, then the user is forced off the port. If there is no user on the port, a setting of TRUE of this variable has no effect. Setting this variable to FALSE has no effect.
Maximum Requests (Modifiable)	Set the maximum number of times EAP request frames will be transmitted to the supplicant before timeout. Default is **2**; range is **1** to **10**.

3.11 EAP STATISTICS MENU SCREEN

Screen Navigation Path

Password > Device Menu > Security Menu > **EAP Statistics Menu**

When to Use

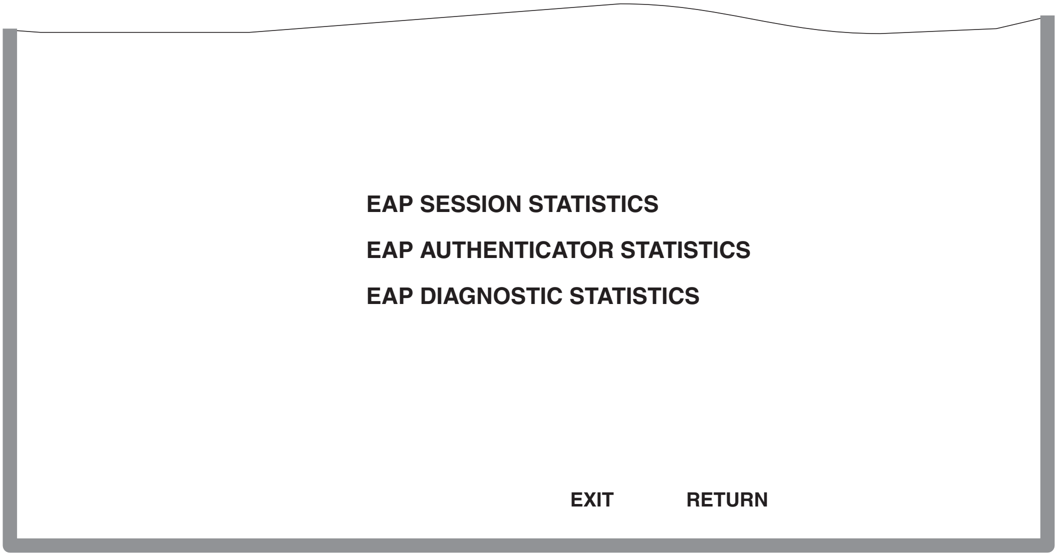
To access the EAP Session Statistics, EAP Authenticator Statistics, and EAP Diagnostic Statistics screens.

How to Access

Use the arrow keys to highlight the **EAP STATISTICS** menu item on the Security Menu screen and press ENTER. The EAP Statistics Menu screen, Figure 3-10, displays.

Screen Example

Figure 3-10 EAP Statistics Menu Screen



3783_04

Menu Descriptions

Refer to Table 3-10 for a functional description of each menu item.

Table 3-10 EAP Statistics Menu Screen Descriptions

Menu Item	Screen Function
EAP SESSION STATISTICS	Used to review and clear EAP session statistics for each port. For details, refer to Section 3.11.1.
EAP AUTHENTICATOR STATISTICS	Used to review authenticator statistics for each port, including EAP frame types received and transmitted, and frame version number and source MAC address. For details, refer to Section 3.11.2.
EAP DIAGNOSTIC STATISTICS	Used to view port counters useful for EAP troubleshooting, including logoffs and timeouts while authenticating, and to view authorization failure messages from the authentication server. For details, refer to Section 3.11.3.

3.11.1 EAP Session Statistics Screen

When to Use

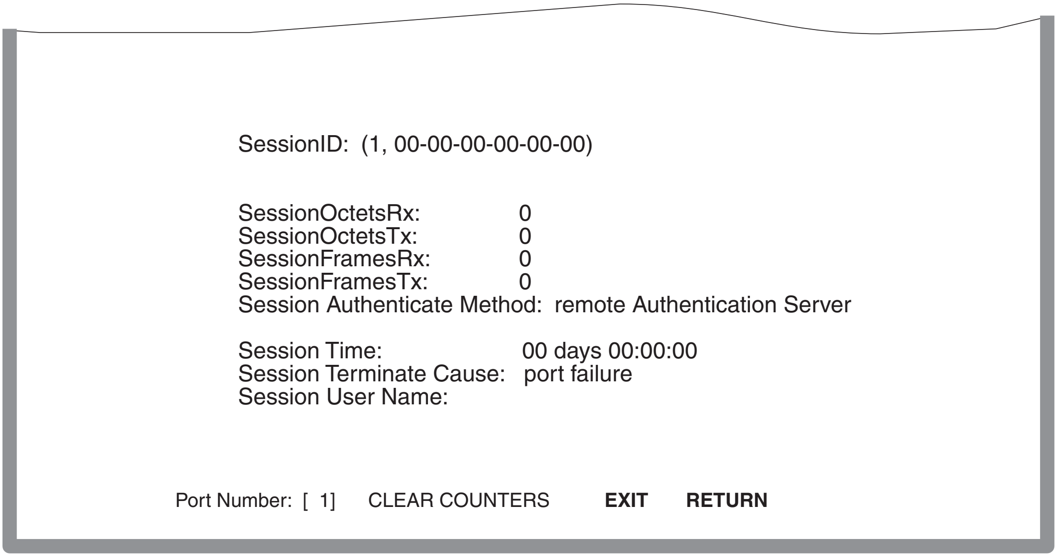
To review and clear EAP session statistics for each port.

How to Access

Use the arrow keys to highlight the **EAP SESSION STATISTICS** menu item on the EAP Statistics Menu screen and press ENTER. The EAP Session Statistics screen, Figure 3-11, displays.

Screen Example

Figure 3-11 EAP Session Statistics Screen



```
SessionID:  (1, 00-00-00-00-00-00)


SessionOctetsRx:              0
SessionOctetsTx:              0
SessionFramesRx:              0
SessionFramesTx:              0
Session Authenticate Method:  remote Authentication Server

Session Time:                 00 days 00:00:00
Session Terminate Cause:      port failure
Session User Name:


Port Number:  [  1]     CLEAR COUNTERS        EXIT      RETURN
```

3783_05

Field Descriptions

Refer to Table 3-11 for a functional description of each screen field.

Table 3-11 EAP Session Statistics Screen Field Descriptions

Use this field…	To…
SessionID (Read-Only)	See the unique ASCII string identifier for a particular session.
SessionOctetsRx (Read-Only)	See counts of user data octets received on the port during a particular session.
SessionOctetsTx (Read-Only)	See counts of octets of transmitted on the port during a particular session.
SessionFramesRx (Read-Only)	See counts of user data received on the port during a particular session.
SessionFramesTx (Read-Only)	See counts of user data frames transmitted on the port during a particular session.
Session Authenticate Method (Read-Only)	See whether the session was established by a **remote Authentication Server** or a **local Authentication Server**.
Session Time (Read-Only)	See the amount of time a session has been active in days, hours, minutes, and seconds.
Session Terminate Cause (Read-Only)	See which of the following reasons ended the session: • **Supplicant Logoff**: End user logged off. • **port failure**: Authentication port failed. • **Supplicant Restart**: End user restarted session. • **Reauthentication Failed**: A previously authenticated Supplicant has failed to re-authenticate successfully following timeout of the reauthentication timer or explicit reauthentication. • **authControlForce Unauth**: Port forced to unauthorize mode by network manager. • **portReInit**: Port reinitialized. • **portAdminDisabled**: Port disabled. • **notTerminatedYet:** Session still active.

Table 3-11 EAP Session Statistics Screen Field Descriptions (Continued)

Use this field…	To…
Session User Name (Read-Only)	See the user name associated with the PAE (Point of Access Entity).
Port Number (Selectable)	Select the port number to display the associated EAP Session Statistics. To select a port number, use the arrow keys to highlight the **Port Number** field. Then step to the correct port number using the SPACE bar and press ENTER to display the associated port EAP Session Statistics.
CLEAR COUNTERS (Command)	Set the octets and frame counters to zero for a particular port. To clear the counters, highlight **CLEAR COUNTERS** and press ENTER. **NOTE:** This command clears the counters for this LM screen, but it does not clear the associated MIB objects.

3.11.2 EAP Authenticator Statistics Screen

When to Use

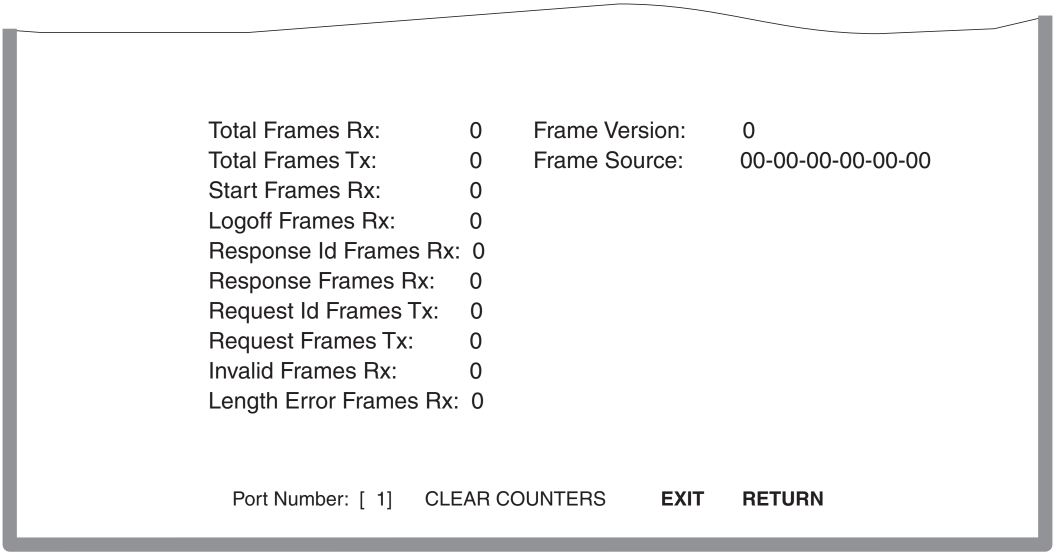
To review authenticator statistics for each port, including EAP frame types received and transmitted, and frame version number and source MAC address. This screen refreshes counters data automatically.

How to Access

Use the arrow keys to highlight the **EAP AUTHENTICATOR STATISTICS** menu item on the EAP Statistics Menu screen and press ENTER. The EAP Authenticator Statistics screen, Figure 3-12, displays.

Screen Example

Figure 3-12 EAP Authenticator Statistics Screen



```
Total Frames Rx:          0      Frame Version:      0
Total Frames Tx:          0      Frame Source:       00-00-00-00-00-00
Start Frames Rx:          0
Logoff Frames Rx:         0
Response Id Frames Rx:    0
Response Frames Rx:       0
Request Id Frames Tx:     0
Request Frames Tx:        0
Invalid Frames Rx:        0
Length Error Frames Rx:   0
```

3783_06

Field Descriptions

Refer to Table 3-12 for a functional description of each screen field.

Table 3-12 EAP Authenticator Statistics Screen Field Descriptions

Use this field…	To…
Total Frames Rx (Read-Only)	See counts of all EAP frames received by the authenticator.
Total Frames Tx (Read-Only)	See counts of all EAP frames transmitted by the authenticator.
Start Frames Rx (Read-Only)	See counts of EAP start type frames received by the authenticator.
Logoff Frames Rx (Read-Only)	See counts of EAP logoff type frames received by the authenticator.

Table 3-12 EAP Authenticator Statistics Screen Field Descriptions (Continued)

Use this field…	To…
Response Id Frames Rx (Read-Only)	See counts of EAP response identification type frames received by the authenticator.
Response Frames Rx (Read-Only)	See counts of EAP response type frames received by the authenticator.
Request Id Frames Tx (Read-Only)	See counts of EAP request identification type frames transmitted by the authenticator.
Request Frames Tx (Read-Only)	See counts of EAP request identification type frames transmitted by the authenticator.
Invalid Frames Rx (Read-Only)	See counts of frames received by the authenticator that have an unrecognizable frame type.
Length Error Frames Rx (Read-Only)	See counts of frames received by the authenticator with an invalid length field for the frame body,
Frame Version (Read-Only)	See the EAP protocol version present in the most recent EAP frame.
Frame Source (Read-Only)	See the source MAC address for the most recent EAP frame received.
Port Number (Selectable)	Select the port number to display the associated EAP Authenticator Statistics. To select a port number, use the arrow keys to highlight the **Port Number** field. Then step to the correct port number using the SPACE bar and press ENTER to display the associated port EAP Authenticator Statistics.
CLEAR COUNTERS (Command)	Set the octets and frame counters to zero for a particular port. To clear the counters, highlight **CLEAR COUNTERS** and press ENTER. **NOTE:** This command clears the counters for this LM screen, but it does not clear the associated MIB objects.

3.11.3 EAP Diagnostic Statistics Screen

When to Use

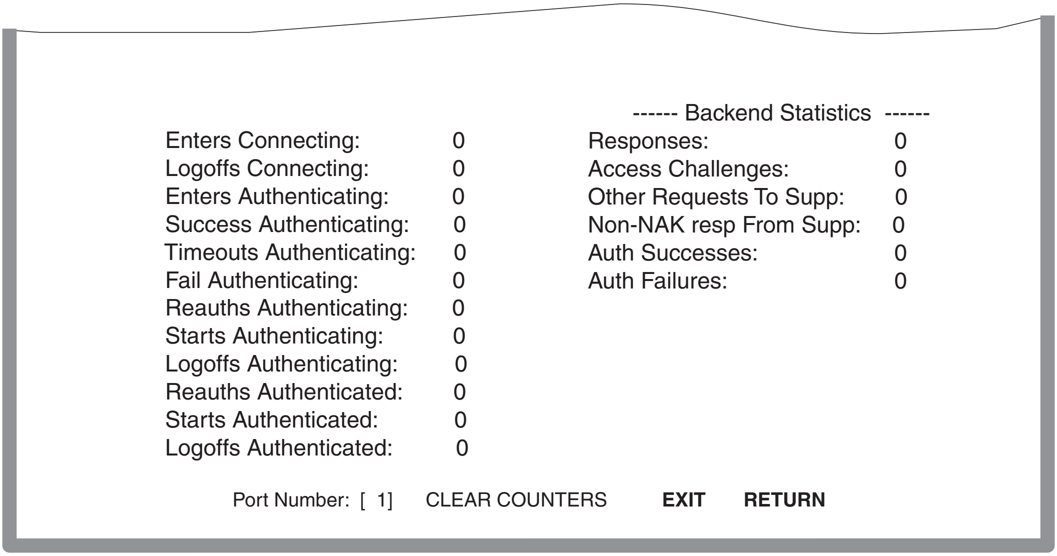
To view port counters useful for EAP troubleshooting, including logoffs and timeouts while authenticating, and to view authorization failure messages from the authentication server. The counters on this screen refresh automatically.

How to Access

Use the arrow keys to highlight the **EAP DIAGNOSTIC STATISTICS** menu item on the EAP Statistics Menu screen and press ENTER. The EAP Diagnostic Statistics screen, Figure 3-13, displays.

Screen Example

Figure 3-13 EAP Diagnostic Statistics Screen



```
                                          ------ Backend Statistics  ------
Enters Connecting:          0        Responses:                  0
Logoffs Connecting:         0        Access Challenges:          0
Enters Authenticating:      0        Other Requests To Supp:     0
Success Authenticating:     0        Non-NAK resp From Supp:     0
Timeouts Authenticating:    0        Auth Successes:             0
Fail Authenticating:        0        Auth Failures:              0
Reauths Authenticating:     0
Starts Authenticating:      0
Logoffs Authenticating:     0
Reauths Authenticated:      0
Starts Authenticated:       0
Logoffs Authenticated:      0

      Port Number:  [  1]    CLEAR COUNTERS      EXIT     RETURN
```

3783_07

Field Descriptions

Refer to Table 3-13 for a functional description of each screen field.

Table 3-13 EAP Diagnostic Statistics Screen Field Descriptions

Use this field…	To…
Enters Connecting (Read-Only)	See counts of transitions to connecting state from any other state.
Logoffs Connecting (Read-Only)	See counts of transitions from connecting to disconnected state after an EAPOL logoff message. EAPOL is an encapsulation of the EAP protocol, plus some extra data fields, within a LAN frame.
Enters Authenticating (Read-Only)	See counts of transitions from connecting to authenticating state after an EAP Respld message is received from the supplicant (end-user requesting authentication).
Success Authenticating (Read-Only)	See counts of transitions from authenticating to authenticated state after backend authentication has a successful authentication with the supplicant (end-user requesting authentication).
Timeouts Authenticating (Read-Only)	See counts of transitions from authenticating to aborting state due to backend authentication timing out.
Fail Authenticating (Read-Only)	See counts of transitions from authenticating to held state due to backend authentication failure.
Reauths Authenticating (Read-Only)	See counts of transitions from authenticating to aborting state due to reauthentication requests.
Starts Authenticating (Read-Only)	See counts of transitions from authenticating to aborting state due to a start from the supplicant (end-user requesting authentication).
Logoffs Authenticating (Read-Only)	See counts of transitions from authenticating to aborting state due to a logoff message from the supplicant (end-user requesting authentication).

Table 3-13 EAP Diagnostic Statistics Screen Field Descriptions (Continued)

Use this field…	To…
Reauths Authenticated (Read-Only)	See counts of transitions from authenticated to connecting state due to a reauthentication request.
Starts Authenticated (Read-Only)	See counts of transitions from authenticated to connecting state due to a start from the supplicant (end-user requesting authentication).
Logoffs Authenticated (Read-Only)	See counts of transitions from authenticating to disconnected state due to a logoff message from the supplicant (end-user requesting authentication).
Backend Statistics:	
Responses (Read-Only)	See counts of initial access-request frames to the authentication server.
Access Challenges (Read-Only)	See counts of initial access-challenge frames to the authentication server.
Other Requests To Supp (Read-Only)	See counts of EAP request frames transmitted that are not EAP notification, failure or success-type messages. This frame count indicates that the authenticator picked an EAP method.
Non-NAK resp From Supp (Read-Only)	See counts of initial responses to an EAP request from the supplicant (end-user requesting authentication). Count does not include EAP-NAK frames. This count indicates that the supplicant can communicate with the chosen EAP method.
Auth Successes (Read-Only)	See counts of EAP success messages from the authentication server. Indicates that the supplicant is successfully authenticated.
Auth Failures (Read-Only)	See counts of EAP failure messages from the authentication server. Indicates that the supplicant is not authenticated.

Table 3-13 EAP Diagnostic Statistics Screen Field Descriptions (Continued)

Use this field…	To…
Port Number (Selectable)	Select the port number to display the associated EAP Diagnostic Statistics. To select a port number, use the arrow keys to highlight the **Port Number** field. Then step to the correct port number using the SPACE bar and press ENTER to display the associated port EAP Diagnostic Statistics.
CLEAR COUNTERS (Command)	Set the octets and frame counters to zero for a particular port. To clear the counters, use the arrow keys to highlight **CLEAR COUNTERS** and press ENTER. **NOTE:** This command clears the counters for this LM screen, but it does not clear the associated MIB objects.

3.12 MAC PORT CONFIGURATION SCREEN

When to Use

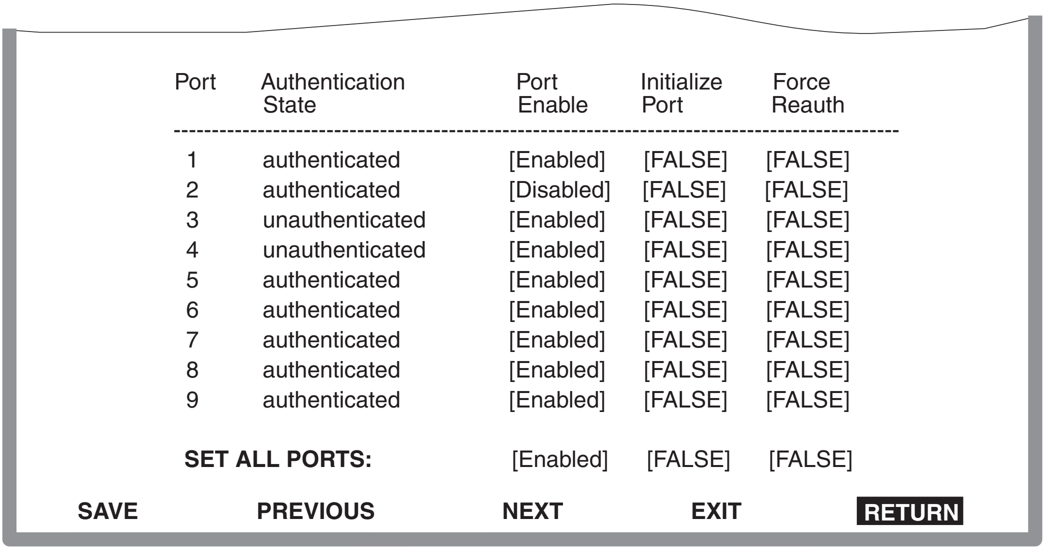
To display the authentication state of the supplicant associated with each port, enable or disable the authentication function, initialize authentication status, and force a revalidation of the MAC credential on a per port basis.

How to Access

Use the arrow keys to highlight the **MAC PORT CONFIGURATION** menu item on the Security Menu screen and press ENTER. The MAC Port Configuration screen, Figure 3-14, displays.

Screen Example

Figure 3-14 MAC Port Configuration Screen



```
Port   Authentication        Port        Initialize   Force
       State                 Enable      Port         Reauth
-------------------------------------------------------------------------
 1     authenticated         [Enabled]   [FALSE]     [FALSE]
 2     authenticated         [Disabled]  [FALSE]     [FALSE]
 3     unauthenticated       [Enabled]   [FALSE]     [FALSE]
 4     unauthenticated       [Enabled]   [FALSE]     [FALSE]
 5     authenticated         [Enabled]   [FALSE]     [FALSE]
 6     authenticated         [Enabled]   [FALSE]     [FALSE]
 7     authenticated         [Enabled]   [FALSE]     [FALSE]
 8     authenticated         [Enabled]   [FALSE]     [FALSE]
 9     authenticated         [Enabled]   [FALSE]     [FALSE]

 SET ALL PORTS:              [Enabled]   [FALSE]     [FALSE]
```

35281_21

Field Descriptions

Refer to Table 3-7 for a functional description of each screen field.

Table 3-14 MAC Port Configuration Screen Field Descriptions

Use this field…	To…
Port # (Read-Only)	See the port numbers of all ports known to the device. Up to 9 ports can be displayed at a time. To see additional ports, select NEXT and press ENTER to display the authentication type and status for the next 10 ports.
Authentication State (Read-Only)	See the current state of the MAC Authentication of a port supplicant. If a supplicant is currently active, on that port, then authenticated is displayed in this field, otherwise unauthenticated is displayed.
Port Enable (Toggle)	Enable or disable the MAC authentication function for a given port.

Table 3-14 MAC Port Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Initialize Port (Single Setting)	Initialize the authentication status of the port. When this field is set to TRUE, the current authentication session is terminated, the port returns to its initial authentication status, and the field returns to **FALSE**.
Force Reauth (Single Setting)	Forces the revalidation of the MAC credential for the port. When this field is set to TRUE, revalidation is executed. When set to **TRUE**, the field returns to **FALSE**. It always reads a value of **FALSE**.
SET ALL PORTS (Command)	Sets all ports in the module to the settings in the associated Port Enable, Initialize Port, and Force Port columns.

3.13 MAC SUPPLICANT CONFIGURATION SCREEN

When to Use

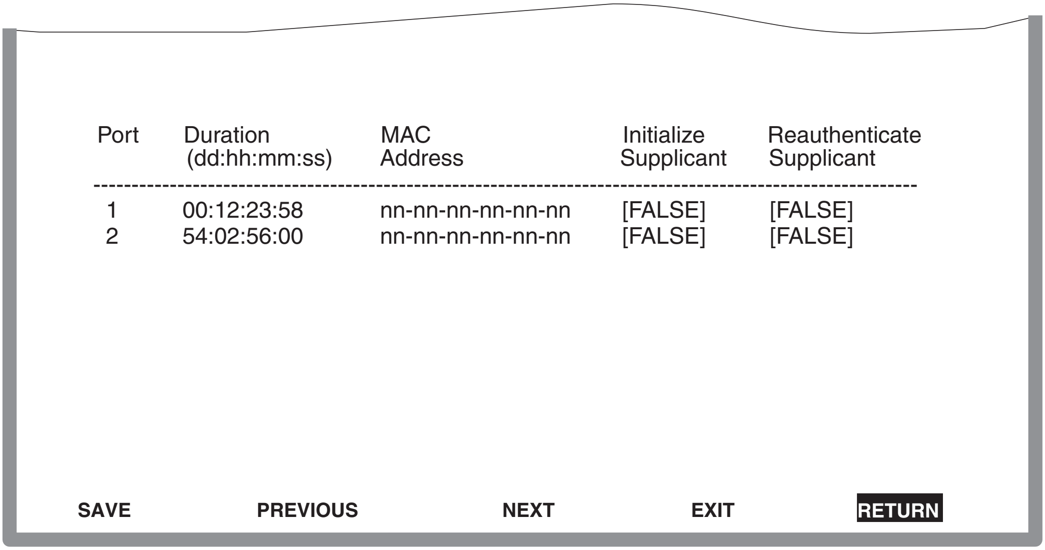
To determine the active MAC Authentication supplicants on the module and perform limited configuration on these supplicants, which includes initializing the supplicant and reauthenticating the supplicant.

How to Access

Use the arrow keys to highlight the **MAC SUPPLICANT CONFIGURATION** menu item on the Security Menu screen and press ENTER. The MAC Supplicant Configuration screen, Figure 3-15, displays.

Screen Example

Figure 3-15 MAC Supplicant Configuration Screen



```
Port    Duration         MAC                      Initialize    Reauthenticate
         (dd:hh:mm:ss)    Address                  Supplicant    Supplicant
--------------------------------------------------------------------------------
 1      00:12:23:58      nn-nn-nn-nn-nn-nn        [FALSE]       [FALSE]
 2      54:02:56:00      nn-nn-nn-nn-nn-nn        [FALSE]       [FALSE]







SAVE          PREVIOUS          NEXT          EXIT          RETURN
```

Field Descriptions

Refer to Table 3-15 for a functional description of each screen field.

Table 3-15 MAC Supplicant Configuration Screen Field Descriptions

Use this field…	To…
Port (Read-Only)	See the port numbers of all ports known to the device. Up to 10 ports can be displayed at a time. To see additional ports, select NEXT and press ENTER to display the authentication type and status for the next 10 ports.
Duration (Read Only)	See the time in days:hours:minutes:seconds that an active supplicant is logged on via the port.
MAC Address (Read Only)	See the ASCII value of the MAC address for each active supplicant associated with a port.

Table 3-15 MAC Supplicant Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Initialize Supplicant (Single Setting)	Terminate the current session with a supplicant. When set to **TRUE**, the current session is terminated. It always displays a value of **FALSE**.
Reauthenticate Supplicant (Single Setting)	Force a revalidation of the MAC credential for the supplicant. When set to **TRUE**, the switch forces the revalidation. It always displays a value of **FALSE**.

4

Device Configuration Menu Screens

This chapter describes the Device Configuration Menu screen and the following screens that can be selected:

- General Configuration screen (Section 4.2)
- SNMP Configuration Menu screen (Section 4.3)
  - SNMP Community Names Configuration screen (Section 4.4)
  - SNMP Traps Configuration screen (Section 4.5)
  - Access Control List screen (Section 4.6)
- System Resources Information screen (Section 4.7)
- FLASH Download Configuration screen (Section 4.8)
- Port Configuration Menu screen (Chapter 5)
- 802.1 Configuration Menu screen (Chapter 6)
- Layer 3 Extensions Menu (Chapter 9)

4.1 DEVICE CONFIGURATION MENU SCREEN

Screen Navigation Path

Password > Device Menu > **Device Configuration Menu**

When to Use

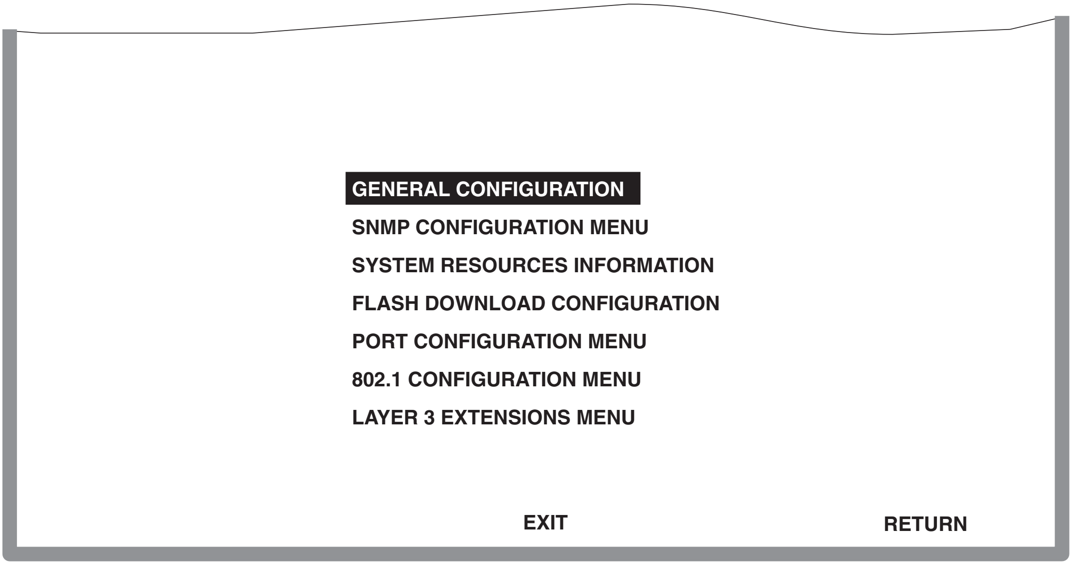
To access a series of Local Management screens used to establish an Access Control List for SNMP to provide additional security, configure and monitor operating parameters, modify SNMP community names, set SNMP traps, configure switch parameters and configure the device ports.

How to Access

Use the arrow keys to highlight the **DEVICE CONFIGURATION MENU** item on the Device Menu screen, and press ENTER. The Device Configuration Menu screen, Figure 4-1, displays.

Screen Example

Figure 4-1 Device Configuration Menu Screen



30691_07

Menu Descriptions

Refer to Table 4-1 for a functional description of each menu item.

Table 4-1 Device Configuration Menu Screen Menu Item Descriptions

Menu Item	Screen Function
GENERAL CONFIGURATION	Used to monitor and configure the device operating parameters. For details, refer to Section 4.2.
SNMP CONFIGURATION MENU	Used to access the SNMP Community Names Configuration, SNMP Traps Configuration, and Access Control List screens. These screens are used to modify SNMP community names, set SNMP traps and provide additional security while managing the device. For details, refer to Section 4.3.
SYSTEM RESOURCES INFORMATION	Displays the CPU type used in the device and its operating speed; displays the size of each memory system used (FLASH memory, DRAM and NVRAM) in the device and the unused portion of each memory; and displays the current CPU (switch) utilization and the peak switch utilization. For details, refer to Section 4.7.
FLASH DOWNLOAD CONFIGURATION	Used to force the device to download a new image file from a TFTP server to its FLASH memory. For details, refer to Section 4.8. To prevent passwords from being downloaded and overwriting the current passwords in memory, refer to the Security screen information described in Section 3.5.
PORT CONFIGURATION MENU	Used to select the screens for configuring the device ports. For details, refer to Section 5.1.
802.1 CONFIGURATION MENU	Provides access to the Spanning Tree Configuration Menu screen, the 802.1Q VLAN Configuration Menu screen, and the 802.1p Priority Configuration Menu screen. For details, refer to Section 6.1.
LAYER 3 EXTENSIONS MENU	Provides access to the IGMP/VLAN Configuration screen to configure ports and VLANs to operate according to the Internet Group Management Protocol (IGMP). For details, refer to Chapter 9.

4.2 GENERAL CONFIGURATION SCREEN

When to Use

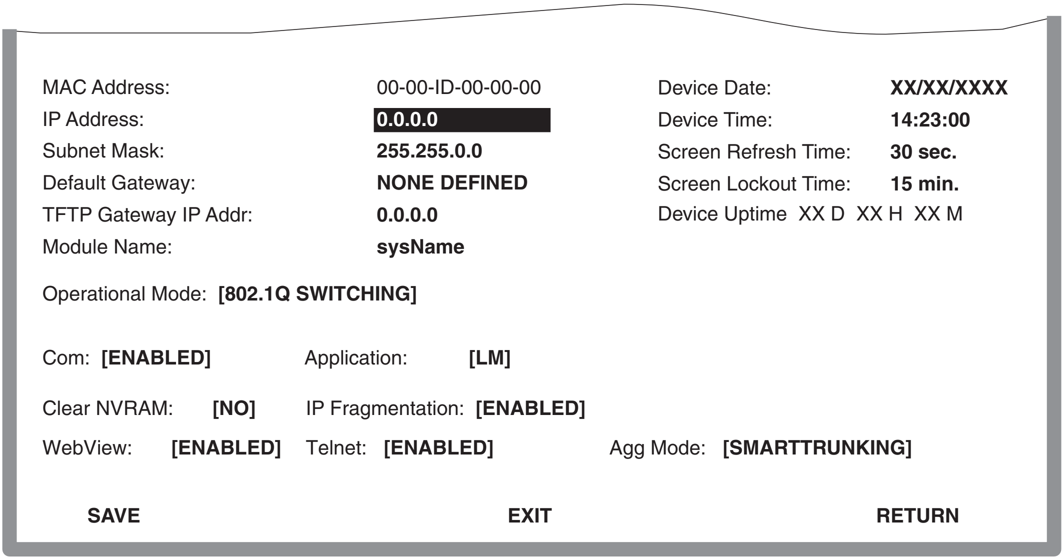
To set the system date and time, IP address and subnet mask, the default gateway, and the TFTP gateway IP address. This screen can also be used to clear the NVRAM, set the screen refresh time, the screen lockout time, the IP fragmentation, the COM port configuration, and monitor the total time (uptime) that the device has been running.

How to Access

Use the arrow keys to highlight the **GENERAL CONFIGURATION** menu item on the Device Configuration Menu screen and press ENTER. The General Configuration screen, Figure 4-2, displays.

Screen Example

Figure 4-2 General Configuration Screen



```
MAC Address:                 00-00-ID-00-00-00      Device Date:            XX/XX/XXXX
IP Address:                  0.0.0.0                Device Time:            14:23:00
Subnet Mask:                 255.255.0.0            Screen Refresh Time:    30 sec.
Default Gateway:             NONE DEFINED           Screen Lockout Time:    15 min.
TFTP Gateway IP Addr:        0.0.0.0                Device Uptime  XX D  XX H  XX M
Module Name:                 sysName

Operational Mode:  [802.1Q SWITCHING]

Com:  [ENABLED]             Application:        [LM]

Clear NVRAM:     [NO]       IP Fragmentation:  [ENABLED]

WebView:     [ENABLED]      Telnet:   [ENABLED]           Agg Mode:   [SMARTTRUNKING]

      SAVE                              EXIT                                  RETURN
```

3650_12_1

Field Descriptions

Refer to Table 4-2 for a functional description of each screen field.

Table 4-2 General Configuration Screen Field Descriptions

Use this field…	To…
MAC Address (Read-Only)	See the base physical address of the device.
IP Address (Modifiable)	See the IP address for the device. To set the IP address, refer to Section 4.2.1. The IP address can also be set through Runtime IP Address Discovery. Runtime IP Address Discovery enables the device to automatically accept an IP address from a Boot Strap Protocol (BootP) server on the network without requiring a user to enter an IP address through Local Management.
Subnet Mask (Modifiable)	See the subnet mask for the device. A subnet mask “masks out” the network bits of the IP address by setting the bits in the mask to 1 when the network treats the corresponding bits in the IP address as part of the network or subnetwork address, or to 0 if the corresponding bit identifies the host. When an IP address is entered in the IP Address field, the Subnet Mask field automatically changes to the default subnet mask for that IP address. For details about how to change the subnet mask from its default value, refer to Section 4.2.2.
Default Gateway (Modifiable)	See the default gateway for the device. This field is not defined until an appropriate value is entered. For details about why and how to set the Default Gateway, refer to Section 4.2.3.
TFTP Gateway IP Addr (Modifiable)	See the TFTP Gateway IP address for the device. To set the TFTP Gateway IP address, refer to Section 4.2.4.
Module Name (Modifiable)	Enter a new system name. To enter a new system name, refer to Section 4.2.5.
Device Date (Modifiable)	Enter a new device date. To enter a new date, refer to Section 4.2.6.

Table 4-2 General Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Device Time (Modifiable)	Enter a new device time. To enter a new time, refer to Section 4.2.7.
Screen Refresh Time (Modifiable)	Enter a new device time. This setting determines how frequently (in seconds) information is updated on the screen. To enter the refresh time, refer to Section 4.2.8.
Screen Lockout Time (Modifiable)	Enter a new lockout time. This is maximum number of minutes that the Local Management application displays a screen while awaiting input or action from a user. For example, if the number 5 is entered in this field, the user has up to five minutes to respond to each of the specified device's Local Management screens. In this example, after five minutes of no input or action, the terminal "beeps" five times, the Local Management application terminates the session, and the display returns to the Local Management Password screen. To enter the screen lockout time, refer to Section 4.2.9.
Device Uptime (Read-Only)	See the total time that the device has been operating.
Operational Mode	Display "802.1Q SWITCHING". This setting cannot be changed.
Com (Toggle)	Enable or disable the COM port. The selection toggles between ENABLED and DISABLED. The default is ENABLED. For details about setting up the COM port, refer to Section 4.2.10.
Application (Toggle)	Set the application that the COM port will support. The field toggles between LM (Local Management) and UPS (Uninterruptible Power Supply). The default is LM. The UPS setting allows the COM port to be used to monitor an American Power Conversion (APC) Uninterruptible Power Supply (UPS). The baud rate setting for LM is automatically sensed. For UPS, the baud rate is automatically set to 2400. For details about how to configure the COM port for various applications, refer to Section 4.2.10.

Table 4-2 General Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Clear NVRAM (Toggle)	Reset NVRAM to the factory default settings. All user-entered parameters, such as IP address and Community Names, are then replaced with the device default configuration settings. For details, refer to Section 4.2.11.
IP Fragmentation (Toggle)	Enable or disable IP Fragmentation. The default setting for this field is ENABLED. If the device is to be bridged to an FDDI ring using an HSIM-F6, IP Fragmentation should be enabled. If IP Fragmentation is disabled, all FDDI frames that exceed the maximum Ethernet frame size are discarded if they are destined for a small frame size port, such as Ethernet, WAN, Gigabit Ethernet, and ATM (at the time of this printing). Even if IP Fragmentation is disabled, large frames will still be forwarded out the ports if necessary. Check the release notes for changes. For details on enabling IP Fragmentation, refer to Section 4.2.12.
WebView (Toggle)	Enable or disable WebView to configure or manage the switch via the HTTP agent. The default setting is ENABLED.
Telnet (Toggle)	Enable or disable the ability to Telnet to the switch to access Local Management. The default setting is ENABLED.
Agg Mode (Toggle)	Select the trunking method that the switch will use to create a trunk consisting of a group of ports to increase the bandwidth between switches. You can select either the Enterasys Networks’ SmartTrunking (Huntgroup) or the IEEE 802.3ad protocol. This field toggles between HUNTGROUP and IEEE8023ad. The default is HUNTGROUP. **NOTE:** When the Agg Mode is set to 8023ad, the Port Configuration menu item SMARTTRUNK CONFIGURATION is replaced with LINK AGGREGATION MENU. This menu screen provides access to other screens to display Port, Aggregator and System information, view and configure all the port-related LACP parameters, and display a summary of all the available aggregators and other related infomation. For more information, refer to Section 5.1.

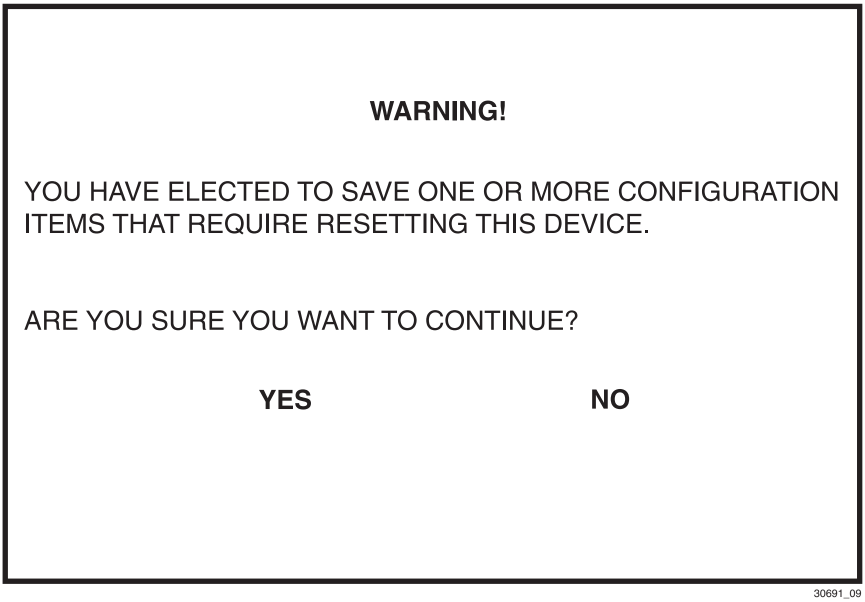
4.2.1 Setting the IP Address

To set the IP address, perform the following steps:

1. Use the arrow keys to highlight the **IP Address** field.
2. Enter the IP address into this field using Dotted Decimal Notation (DDN) format.

   For example: *nnn.nnn.nnn.nnn*
3. Press ENTER. If the IP address is a valid format, the cursor returns to the beginning of the IP address field. If the entry is not valid, the screen displays the message “INVALID IP ADDRESS OR FORMAT ENTERED”. Local Management does not alter the current value and refreshes the IP address field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The warning screen shown in Figure 4-3 displays.

Figure 4-3 Configuration Warning Screen, IP Address



WARNING!

YOU HAVE ELECTED TO SAVE ONE OR MORE CONFIGURATION ITEMS THAT REQUIRE RESETTING THIS DEVICE.

ARE YOU SURE YOU WANT TO CONTINUE?

5. Use the arrow keys to highlight the **YES** command, then press ENTER. The changes are saved and the device reboots.

4.2.2 Setting the Subnet Mask

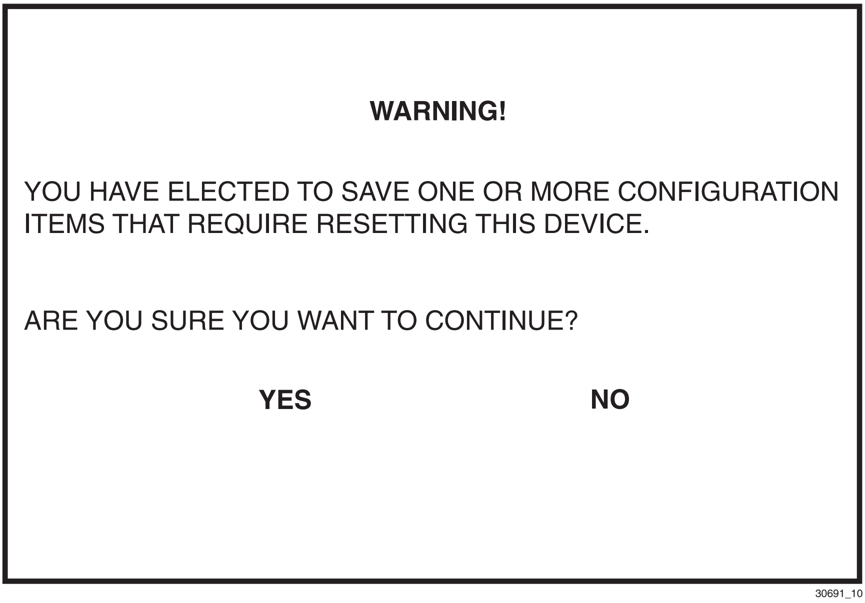
If the management workstation that is to receive SNMP traps from the device is located on a separate subnet, the subnet mask for the device may need to be changed from its default value.

To change the subnet mask from its default, perform the following steps:

1. Use the arrow keys to highlight the **Subnet Mask** field.
2. Enter the subnet mask into this field using Dotted Decimal Notation (DDN) format.

   For example: 255.255.0.0
3. Press ENTER. If the subnet mask is valid, the cursor returns to the beginning of the Subnet Mask field. If the entry is not valid, the screen displays the message “INVALID SUBNET MASK OR FORMAT ENTERED”. Local Management does not alter the current value, but it does refresh the Subnet Mask field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The warning screen shown in Figure 4-4 displays.

Figure 4-4 Configuration Warning Screen, Subnet Mask



WARNING!

YOU HAVE ELECTED TO SAVE ONE OR MORE CONFIGURATION ITEMS THAT REQUIRE RESETTING THIS DEVICE.

ARE YOU SURE YOU WANT TO CONTINUE?

5. Use the arrow keys to highlight the **YES** command, then press ENTER. The changes are saved and the device reboots.

4.2.3 Setting the Default Gateway

If the SNMP management station is located on a different IP subnet than the device, a default gateway must be specified. When an SNMP Trap is generated, the device sends out an ARP request to the default gateway, which responds with its MAC address. The device then sends the trap using the IP address from the Trap Table and the MAC address of the default gateway. To set the default gateway, perform the following steps:

1. Use the arrow keys to highlight the **Default Gateway** field.
2. Enter the IP address of the default gateway using the DDN format.

   For example: *nnn.nnn.nnn.nnn*
3. Press ENTER. If the default gateway entered is in the correct format, the cursor returns to the beginning of the Default Gateway field. If the format is not correct, the screen displays “INVALID DEFAULT GATEWAY OR FORMAT ENTERED”. Local Management does not alter the current value, but it does refresh the Default Gateway field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command.
5. Press ENTER. The message “SAVED OK” displays at the top of the screen.

4.2.4 Setting the TFTP Gateway IP Address

If the network TFTP server is located on a different IP subnet than the device, a Gateway IP address should be specified. To set the TFTP Gateway IP address, perform the following steps:

1. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field.
2. Enter the IP address of the TFTP gateway using the DDN format.

   For example: *nnn.nnn.nnn.nnn*
3. Press ENTER. If the TFTP gateway IP address entered is a valid format, the cursor returns to the beginning of the TFTP Gateway IP Address field. If the entry is not valid, the screen displays “INVALID TFTP GATEWAY IP ADDRESS OR FORMAT ENTERED”. Local Management does not alter the current value, but it does refresh the TFTP Gateway IP Address field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command.
5. Press ENTER. The message “SAVED OK” displays.

4.2.5 Setting the Module Name

To set the module name, perform the following steps:

1. Use the arrow keys to highlight the **Module Name** field.
2. Enter the name of your system (maximum of 19 characters).
3. Press ENTER to set the name in the input field.
4. Use the arrow keys to highlight the **SAVE** command and press ENTER. The message "SAVED OK" displays on the screen.

4.2.6 Setting the Device Date

The device is year 2000 compliant so that the Device Date field can be set beyond the year 1999.

To set the system date, perform the following steps:

1. Use the arrow keys to highlight the **Device Date** field.
2. Enter the date in this format: MM/DD/YYYY

NOTE: It is not necessary to add separators between month, day, and year numbers, as long as each entry has the correct number of numeric characters. For example, to set the date to 03/17/2000, type "03172000" in the Device Date field.

3. Press ENTER to set the system calendar to the date in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the date entered is a valid format, the message displays "SAVED OK" at the top of the screen. If the entry is not valid, Local Management does not alter the current value, but it does refresh the Device Date field with the previous value.

4.2.7 Setting the Device Time

To set the device time, perform the following steps:

1. Use the arrow keys to highlight the **Device Time** field.
2. Enter the time in this 24-hour format: HH:MM:SS

NOTE: When entering the time in the system time field, separators between hours, minutes, and seconds are not needed as long as each entry uses two numeric characters. For example, to set the time to 6:45 P.M., type “184500” in the Device Time field.

3. Press ENTER to set the system clock to the time in the input field.

4.2.8 Entering a New Screen Refresh Time

The screen refresh time can be set from 3 to 99 seconds with a default of 3 seconds. To set a new screen refresh time, perform the following steps:

1. Use the arrow keys to highlight the **Screen Refresh Time** field.
2. Enter a number from 3 to 99.
3. Press ENTER to set the refresh time to the time entered in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is within the 3 to 99 seconds range, the message “SAVED OK” displays at the top of the screen. If the entry is not valid, Local Management does not alter the current setting, but it does refresh the Screen Refresh Time field with the previous value.

4.2.9 Setting the Screen Lockout Time

The screen lockout time can be set from 1 to 30 minutes with a default of 15 minutes. To set a new lockout time, perform the following steps:

1. Use the arrow keys to highlight the **Screen Lockout Time** field.
2. Enter a number from 1 to 30.
3. Press ENTER to set the lockout time in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is within the 1 to 30 minutes range, the message “SAVED OK” displays at the top of the screen. If the entry is not valid, Local Management does not alter the current setting, but it does refresh the Screen Lockout Time field with the previous value.

4.2.10 Configuring the COM Port

Upon power up, the COM port is configured to the default settings of **ENABLED** and **LM**.

CAUTION: Before altering the COM port settings, ensure that the device is set with a valid IP address. (Refer to Section 4.2.1.) Read this entire COM port configuration section before changing the settings of the COM port.

The COM port supports the following applications:

- Local Management connections
- American Power Conversion (APC) Uninterruptible Power Supply (UPS) connections

To configure the COM port, proceed as follows:

1. Use the arrow keys to highlight the **Com** field.

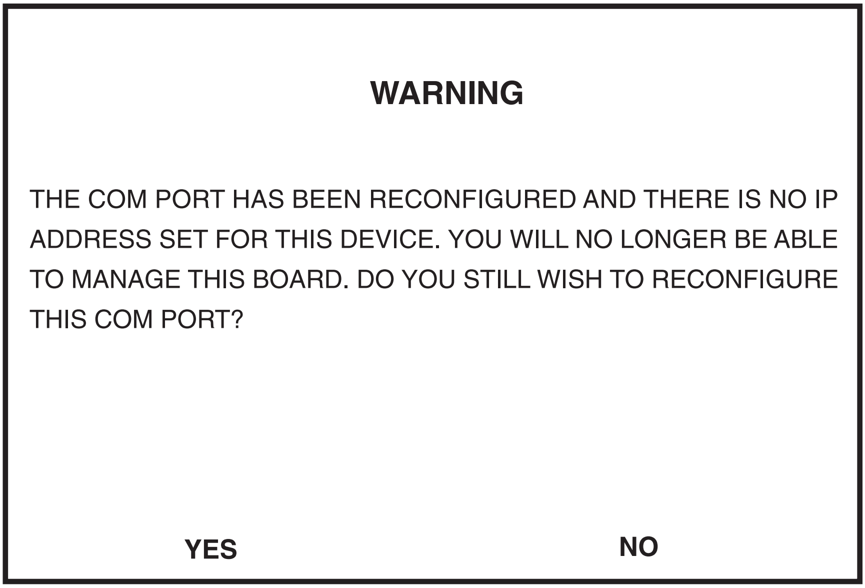
CAUTION: Do **NOT** disable or alter the settings of the COM port while operating the current Local Management connection through a terminal. Altering the COM port settings disconnects the Local Management terminal from the port, and ends the Local Management session. If the device was previously assigned a valid IP address, reenter Local Management by establishing a Telnet connection to the device. If the device does not have a valid IP address and the COM port has been disabled or the settings changed, reset NVRAM on the device using Mode Switch 7 to reestablish COM port communications. For details about Switch 7 and its operation. refer to the device installation user’s guide shipped with your device.

2. Press the SPACE bar to choose either **ENABLED** or **DISABLED**. The COM port must be **ENABLED** for the LM or UPS application. Selecting **DISABLED** prevents the COM port connection to the terminal, providing additional device security.

CAUTION: If the COM port is reconfigured without a valid IP address set on the device, the message shown in Figure 4-5 displays.

Do not continue unless the outcome of the action is fully understood.

Figure 4-5 COM Port Warning



WARNING

THE COM PORT HAS BEEN RECONFIGURED AND THERE IS NO IP ADDRESS SET FOR THIS DEVICE. YOU WILL NO LONGER BE ABLE TO MANAGE THIS BOARD. DO YOU STILL WISH TO RECONFIGURE THIS COM PORT?

YES NO

3. Use the arrow keys to highlight **YES**. Press ENTER.
4. If the port was **ENABLED**, the message “SAVED OK” appears, and the edits are saved. If the port was **DISABLED**, use the arrow keys to highlight **SAVE** at the bottom of the screen, then press ENTER.

NOTE: Exiting without saving causes the message “NOT SAVED -- PRESS SAVE TO KEEP CHANGES” to appear. Exiting without saving causes all edits to be lost.

4.2.10.1 Changing the COM Port Application

After enabling the COM port as described in Section 4.2.10, one of the applications supported by the COM port (LM or UPS) can be selected. The default application is LM.

To change the COM port application:

1. Use the arrow keys to highlight the **Application** field.
2. Use the SPACE bar or BACKSPACE key to step to the desired setting. Table 4-3 lists the available settings and their corresponding applications.

Table 4-3 COM Port Application Settings

Setting	Application
LM	Local Management Session
UPS	APC Power Supply SNMP Proxy

3. Press ENTER to accept the application.

CAUTION: When the COM port is configured to perform the UPS application, all future Local Management connections must be made by establishing a Telnet connection to the device. Ensure that the device has a valid IP address before saving changes to the COM port application. If the device does not have a valid IP address and the changes are saved, refer to your device installation user's guide for instructions on clearing NVRAM to reestablish COM port communications.

4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen, then press the ENTER key. The message "SAVED OK" displays, indicating that the edits are saved.

4.2.11 Clearing NVRAM

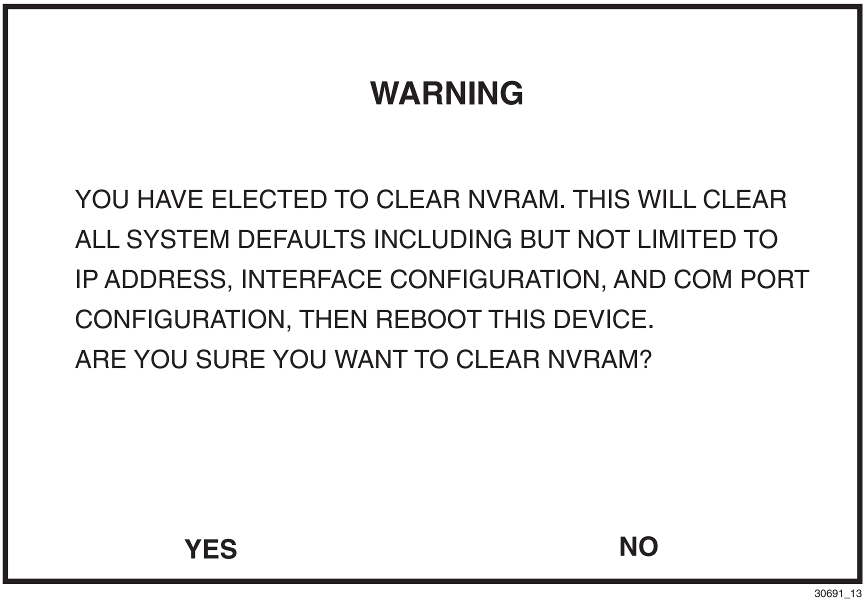
CAUTION: Clearing NVRAM results in the loss of all user-entered parameters. Do not proceed unless the following procedure is completely understood.

Clearing NVRAM is used to clear all user-entered parameters, such as the IP address and Community Names from NVRAM.

To clear NVRAM, proceed as follows:

1. Use the arrow keys to highlight the **Clear NVRAM** field.
2. Use the SPACE bar to toggle the field to **YES**.
3. Use the arrow keys to highlight **SAVE** at the bottom of the screen.
4. Press ENTER. The warning shown in Figure 4-6 displays.

Figure 4-6 Clear NVRAM Warning



WARNING

YOU HAVE ELECTED TO CLEAR NVRAM. THIS WILL CLEAR ALL SYSTEM DEFAULTS INCLUDING BUT NOT LIMITED TO IP ADDRESS, INTERFACE CONFIGURATION, AND COM PORT CONFIGURATION, THEN REBOOT THIS DEVICE.
ARE YOU SURE YOU WANT TO CLEAR NVRAM?

5. To clear the NVRAM, use the arrow keys to select **YES** and press ENTER. The message “CLEARING NVRAM. REBOOT IN PROGRESS...” displays. The device clears NVRAM and reboots. All user-entered parameters default to factory default settings.

4.2.12 Enabling/Disabling IP Fragmentation

To enable or disable IP Fragmentation, proceed as follows:

CAUTION: If the device is being bridged to an FDDI ring (for example, via an optional HSIM-F6), IP Fragmentation should be enabled. If it is disabled, all FDDI frames that exceed the maximum Ethernet frame size are discarded.

1. Use the arrow keys to highlight the **IP Fragmentation** field.
2. Press the SPACE bar to choose either **ENABLED** or **DISABLED**.
3. Use the arrow keys to highlight the **SAVE** command.
4. Press ENTER. The message “SAVED OK” displays.

4.3 SNMP CONFIGURATION MENU SCREEN

Screen Navigation Path

Password > Device Menu > Device Configuration Menu > **SNMP Configuration Menu**

When to Use

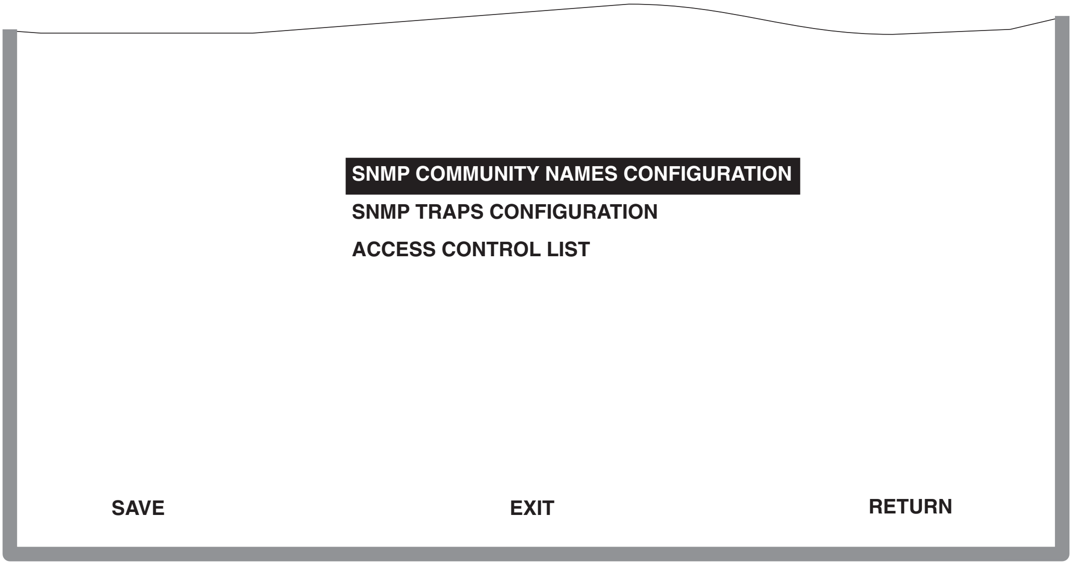
To provide access to the SNMP Community Names Configuration, SNMP Traps Configuration, and Access Control List screens. These screens are used to modify SNMP community names, set SNMP traps, and establish an Access Control List to provide additional security.

How to Access

Use the arrow keys to highlight the **SNMP CONFIGURATION MENU** item on the Device Configuration Menu screen, and press ENTER. The SNMP Configuration Menu screen, Figure 4-7, displays.

Screen Example

Figure 4-7 SNMP Configuration Menu Screen



30691_14

Menu Descriptions

Refer to Table 4-4 for a functional description of each menu item.

Table 4-4 SNMP Configuration Menu Screen Menu Item Descriptions

Menu Item	Screen Function
SNMP COMMUNITY NAMES CONFIGURATION	Used to enter new, change, or review the community names used as access passwords for device management operation. Access is limited based on the password level of the user. For details, refer to Section 4.4.
SNMP TRAPS CONFIGURATION	Provides display and configuration access to the table of IP addresses used for trap destinations and associated community names. For details, refer to Section 4.5.
ACCESS CONTROL LIST	Enables the system administrator to create an Access Control List (ACL) to restrict device access to a maximum of 16 single IP addresses and/or ranges of IP addresses. For details, refer to Section 4.6.

4.4 SNMP COMMUNITY NAMES CONFIGURATION SCREEN

When to Use

To set SNMP Management community names. Community names provide multiple levels of manageability and are agents of security access to the device. Access is controlled by enacting any of three different levels of security authorization (read-only, read-write, and super-user).

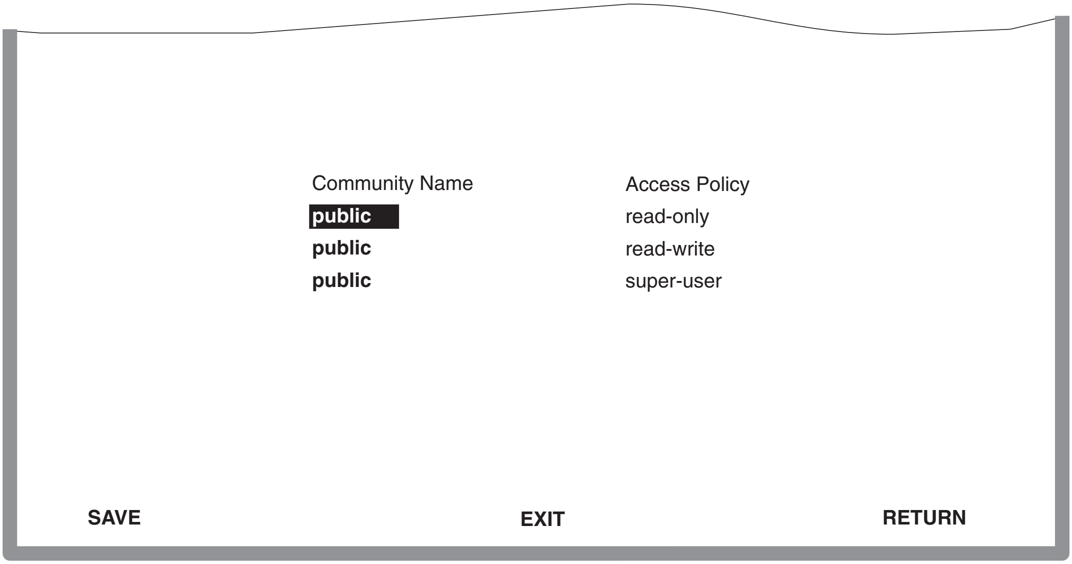
NOTE: Super-user access gives the user full management privileges, allows existing passwords to be changed, and all modifiable MIB objects to be edited.

How to Access

Use the arrow keys to highlight the **SNMP COMMUNITY NAMES CONFIGURATION** menu item on the SNMP Configuration Menu screen and press ENTER. The SNMP Community Names Configuration screen, Figure 4-8, displays.

Screen Example

Figure 4-8 SNMP Community Names Configuration Screen



Community Name	Access Policy
public	read-only
public	read-write
public	super-user

NOTE: As typical in secure network environments, the community name fields are masked from view with asterisk (*).

Field Descriptions

Refer to Table 4-5 for a functional description of each screen field.

Table 4-5 SNMP Community Names Configuration Screen Field Descriptions

Use this field…	To…
Community Name (Modifiable)	Enter the user-defined name through which a user accesses the device SNMP Management. Any community name assigned here acts as a password to Local Management.

Table 4-5 SNMP Community Names Configuration Screen Field Descriptions (Continued)

Use this field…	To…	
Access Policy (Read-Only)	Indicate the access accorded each community name. The available access levels are as follows:	
	read-only	This community name gives the user read-only access to the device MIB objects, and excludes access to security-protected fields of read-write or super-user authorization.
	read-write	This community name gives the user read-write access to the device MIB objects, excluding security protected fields for Super-User access only.
	super-user	This community name gives the user read-write access to the device MIB objects and allows the user to change all modifiable parameters including community names, IP addresses, traps, and SNMP objects.

4.4.1 Establishing Community Names

The password used to access Local Management at the Password Screen must have super-user access to view and edit the SNMP Community Names Configuration screen. Using a password with read-only or read-write access does not allow the viewing or editing of the SNMP Community Names Configuration screen.

To establish community names, proceed as follows:

1. Use the arrow keys to highlight the **Community Name** field adjacent to the selected access level.
2. Enter the password in the field (maximum 32 characters).
3. Press ENTER.
4. Repeat steps 1 through 3 to modify the other community names.
5. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER. The message “SAVED OK” displays. The community names are saved to memory and their access modes implemented.

NOTE: Exiting without saving causes a “NOT SAVED?” message to display at the top left of the screen. Edits are lost if they are not saved before exiting.

4.5 SNMP TRAPS CONFIGURATION SCREEN

When to Use

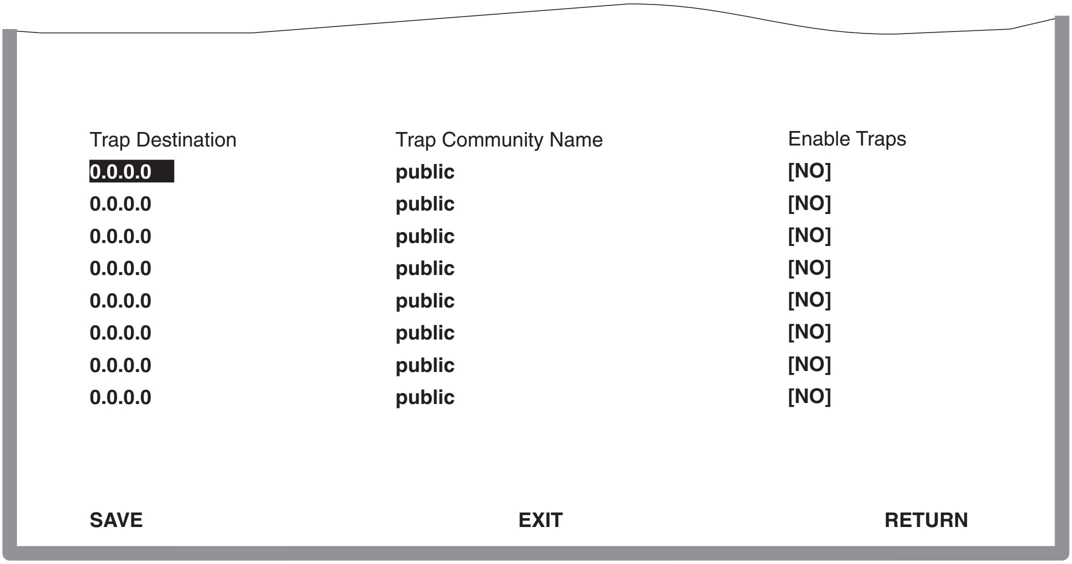
To assign SNMP traps to eight different IP addresses. Since the device is an SNMP compliant device, it can send messages to multiple Network Management Stations to alert users of status changes.

How to Access

Use the arrow keys to highlight the **SNMP TRAPS CONFIGURATION** menu item on the SNMP Configuration Menu screen, and press ENTER. The SNMP Traps Configuration screen, Figure 4-9, displays.

Screen Example

Figure 4-9 SNMP Traps Configuration Screen



```
Trap Destination          Trap Community Name          Enable Traps
0.0.0.0                   public                       [NO]
0.0.0.0                   public                       [NO]
0.0.0.0                   public                       [NO]
0.0.0.0                   public                       [NO]
0.0.0.0                   public                       [NO]
0.0.0.0                   public                       [NO]
0.0.0.0                   public                       [NO]
0.0.0.0                   public                       [NO]
```

Field Descriptions

Refer to Table 4-6 for a functional description of each screen field.

Table 4-6 SNMP Traps Configuration Screen Field Descriptions

Use this field…	To…
Trap Destination (Modifiable)	Display/enter the IP address of the workstation to receive trap alarms. Up to eight different destinations can be defined.
Trap Community Name (Modifiable)	Display/enter the Trap Community Name included in the trap message along with the IP address of the Network Management Station to receive the trap alarm.
Enable Traps (Toggle)	Enable/disable the transmission of traps to the network management station with the associated IP address. This field toggles between YES and NO.

4.5.1 Configuring the Trap Table

To configure the Trap table, proceed as follows:

1. Use the arrow keys to highlight the appropriate **Trap Destination** field.
2. Enter the IP address of the workstation that is to receive traps. IP address entries must follow the DDN format.

   For example: *nnn.nnn.nnn.nnn*
3. Press ENTER. If an invalid entry is entered, the message “INVALID IP ENTERED” displays in the Event Message Line.
4. Use the arrow keys to highlight the **Trap Community Name** field. Enter the community name.
5. Press ENTER.
6. Use the arrow keys to highlight the **Enable Traps** field. Press the SPACE bar to choose either **YES** (send alarms from the device to the workstation), or **NO** (prevent alarms from being sent).
7. Use the arrow keys to highlight the **SAVE** command and press ENTER. The message “SAVED OK” displays on the screen.

NOTE: Exiting without saving causes a “NOT SAVED?” message to appear above the **SAVE** command. Edits are lost if they are not saved before exiting.

The designated workstations will now receive traps from the device as long as the communication path to the designated workstations is not inhibited (for example, by subnets or VLANs).

4.6 ACCESS CONTROL LIST SCREEN

When to Use

To view, enable, or disable the Access Control List (ACL) and configure address filtering to provide additional security. This enables you to limiting user to the device according to their IP address. Up to 16 single IP addresses and/or range of addresses can be configured. To manage an ACL enabled device, the management station must be a member of the ACL and authenticated according to traditional SNMP rules.

NOTE: Clearing NVRAM will remove all IP address entries and return the access control state to DISABLED.

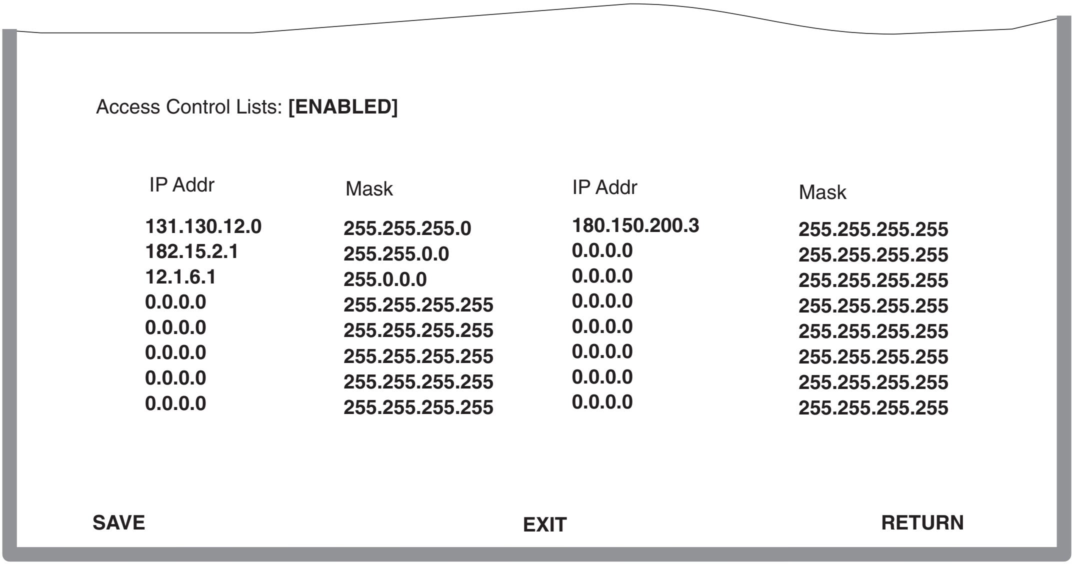
When the ACL is disabled, host access is not restricted.

How to Access

Use the arrow keys to highlight the **ACCESS CONTROL LIST** menu item on the SNMP Configuration Menu screen, and press ENTER. The Access Control List screen, Figure 4-10, displays.

Screen Example

Figure 4-10 Access Control List Screen



```
      Access Control Lists: [ENABLED]

         IP Addr          Mask               IP Addr          Mask

         131.130.12.0     255.255.255.0      180.150.200.3    255.255.255.255
         182.15.2.1       255.255.0.0        0.0.0.0          255.255.255.255
         12.1.6.1         255.0.0.0          0.0.0.0          255.255.255.255
         0.0.0.0          255.255.255.255    0.0.0.0          255.255.255.255
         0.0.0.0          255.255.255.255    0.0.0.0          255.255.255.255
         0.0.0.0          255.255.255.255    0.0.0.0          255.255.255.255
         0.0.0.0          255.255.255.255    0.0.0.0          255.255.255.255
         0.0.0.0          255.255.255.255    0.0.0.0          255.255.255.255


      SAVE                          EXIT                          RETURN
```

3528_01_108

Field Descriptions

Refer to Table 4-7 for a functional description of each screen field.

Table 4-7 Access Control List Screen Field Descriptions

Use this field…	To…
Access Control Lists (Toggle)	Enable or disable ACL to restrict SNMP/IP access to a limited number of IP addresses. This field toggles between ENABLED and DISABLED. DISABLED is the default setting. When ACL is enabled, all device access is limited to the single 16 IP addresses and/or range of IP addresses as shown in the previous screen example (Figure 4-10). The limited access applies to all IP access including, but not limited to, SLIP/PPP connections, Telnet, Ping, SNMP and HTTP. When locally connected to the COM port of the host device, ACL does not restrict access to local management. ACL cannot be enabled unless a valid IP address is listed. When ACL is disabled, host access is not restricted to the devices with an IP address in the Access Control List.
IP Addr (Modifiable)	Enter a new IP address of the devices that you want to have access to SNMP/IP management. The default value is “0.0.0.0”. Up to 16, individual user IP addresses and/or range of user IP addresses can be entered. For individual IP address settings, the mask value must be “255.255.255.255”. For a range of IP addresses, both the IP address and appropriate Mask value must be entered to indicate the range of IP addresses. Only a user with a Super User status can view and modify the ACL. **NOTE:** Clearing NVRAM will remove all IP address entries and return the access control state to DISABLED. For details on entering IP addresses, refer to Section 4.6.1.

Table 4-7 Access Control List Screen Field Descriptions (Continued)

Use this field…	To…
Mask (Modifiable)	Enter a mask value to establish an IP address range based on the IP address in the associated IP address field. For example, in the screen example in Figure 4-10, the IP address and Mask entries 182.15.2.1 and 255.255.0.0 sets the switch module to allow access to all users with addresses starting with 182.15.x.x (x = I don't care.) Address ranges may overlap without any consequences. The default value is "255.255.255.255". For details, refer to Section 4.6.1.

4.6.1 Entering IP Addresses

To enter a single or range of IP addresses into the ACL, proceed as follows:

Entering Single Addresses

1. Use the arrow keys to highlight one of the place holders (**0.0.0.0**) under IP Addresses.
2. Enter the IP address of a device that you want to have access to Local Management using the following format: *nnn.nnn.nnn.nnn* (where *n* is an alphanumeric character).
3. In the adjacent Mask column, the value must be the default value of 255.255.255.255. If not, use the arrow keys to highlight the Mask field and type in: 255.255.255.255
4. Repeat steps 1 through 3 if more than one single address is being entered. Up to 16 IP addresses including those used for entering IP address ranges. If an invalid format is used to enter an IP address, the message "INVALID IP FORMAT ENTERED" displays in the Event Message Line. Then the field returns to 0.0.0.0.
5. Use the arrow keys to highlight the **Access Control Lists** field.
6. Press the SPACE bar to toggle the field to ENABLED.
7. Press ENTER.
8. Use the arrow keys to highlight the **SAVE** command and press ENTER. The message "SAVED OK" displays on the screen.

NOTE: Exiting without saving causes a "NOT SAVED?" message to display above the **SAVE** command. Edits are lost if they are not saved before exiting.

The designated devices associated with the IP addresses in the ACL will now be the only ones to have remote access to Local Management. Access to Local Management using the COM port is not affected.

Entering Ranges of Addresses

1. Use the arrow keys to highlight one of the place holders (0.0.0.0) under IP Addresses.
2. Enter the IP address of a device that you want to have access to Local Management using the following format: *nnn.nnn.nnn.nnn* (where *n* is an alphanumeric character).
3. Use the arrow keys to highlight the Mask field and type in the appropriate Mask value to establish a range of addresses based on the IP address entered. For example, if an IP address of 123.123.20.25 and a mask value of 255.0.0.0 was entered, all IP addresses starting with 123 would have access to Local Management.
4. Repeat steps 1 through 3 if more than one range of addresses is being entered. Up to 16 ranges of IP addresses, including any single IP Addresses entered. If an invalid format is used to enter an IP address, one of the following messages may display in the Event Message Line:

- “INVALID IP FORMAT” if more than 3 periods are entered.
- “INVALID IP” if numbers greater than 255 are entered.
- “DUPLICATE IP” if a duplicate IP address is entered.
- “INTERNAL IP” if the IP of the device is entered.

Then the field returns to 0.0.0.0.

5. Use the arrow keys to highlight the **Access Control Lists** field.
6. Press the SPACE bar to toggle the field to ENABLED.
7. Press ENTER.
8. Use the arrow keys to highlight the **SAVE** command and press ENTER. The message “SAVED OK” displays on the screen.

NOTE: Exiting without saving causes a “NOT SAVED?” message to display above the **SAVE** command. Edits are lost if they are not saved before exiting.

The designated devices associated with the range of IP addresses in the ACL will now have remote access to Local Management. Access to Local Management using the COM port is not affected.

4.6.2 Enable/Disable ACL

To just enable or disable ACL, proceed as follows:

1. Use the arrow keys to highlight the **Access Control Lists** field.
2. Press the SPACE bar to toggle the field to either ENABLED or DISABLED.
3. Press ENTER.
4. Use the arrow keys to highlight the **SAVE** command and press ENTER. The message “SAVED OK” displays on the screen.

NOTE: Exiting without saving causes a “NOT SAVED?” message to display above the **SAVE** command. Edits are lost if they are not saved before exiting.

4.7 SYSTEM RESOURCES INFORMATION SCREEN

When to Use

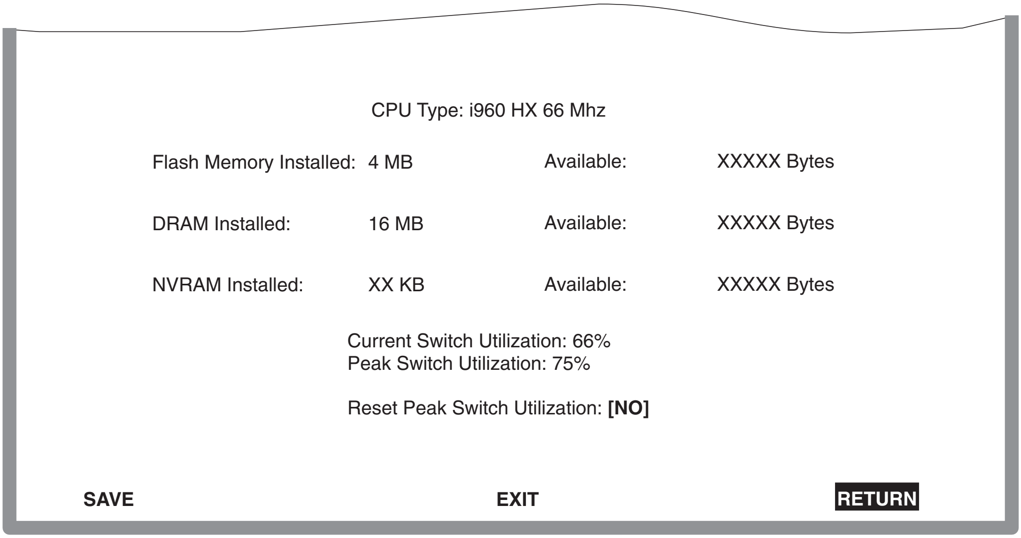
To monitor the current switch utilization and the peak switch utilization. This screen provides information concerning the processor used in the device and the amount of FLASH memory, DRAM, and NVRAM that is installed and how much of that memory is available.

How to Access

Use the arrow keys to highlight the **SYSTEM RESOURCES INFORMATION** menu item on the Device Configuration Menu screen, and press ENTER. The System Resources Information screen, Figure 4-11, displays.

Screen Example

Figure 4-11 System Resources Information Screen



```
                        CPU Type: i960 HX 66 Mhz

Flash Memory Installed:  4 MB        Available:        XXXXX Bytes

DRAM Installed:          16 MB       Available:        XXXXX Bytes

NVRAM Installed:         XX KB       Available:        XXXXX Bytes

                     Current Switch Utilization: 66%
                     Peak Switch Utilization: 75%

                     Reset Peak Switch Utilization: [NO]
```

Field Descriptions

Refer to Table 4-8 for a functional description of each screen field.

Table 4-8 System Resources Information Screen Field Descriptions

Use this field…	To…
CPU Type (Read-Only)	See which microprocessor is used in the device.
Flash Memory Installed (Read-Only)	See the amount of FLASH memory that is installed in the device and how much is currently available.
DRAM Installed (Read-Only)	See the amount of DRAM installed in the device and how much of it is currently available.
NVRAM Installed (Read-Only)	See the amount of NVRAM that is installed in the device and how much of it is currently available.
Current Switch Utilization (Read-Only)	See what percentage of the device switching capacity is currently being used.
Peak Switch Utilization (Read-Only)	See the peak percentage of device switching capacity used, since the last reset.
Reset Peak Switch Utilization (Toggle)	Reset the Peak Switch Utilization field. The switch may be set to either YES or NO as described in Section 4.7.1. YES resets the Peak Switch Utilization field to the current system utilization.

4.7.1 Setting the Reset Peak Switch Utilization

To set the Reset Peak Switch Utilization field to YES or NO, proceed as follows:

1. Use the arrow keys to highlight the **Reset Peak Switch Utilization** field.
2. Press the SPACE bar to select **YES** or **NO**.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays and the Reset Peak Utilization counter resets to zero.

4.8 FLASH DOWNLOAD CONFIGURATION SCREEN

When to Use

To perform the following:

- Download a new firmware image file from a TFTP server to the device,
- Download a configuration file from a TFTP server to the device, or
- Upload the configuration file from the device to a TFTP server.

NOTE: You can also force an image download by changing the position of Switch 6 located inside the device. Use this as a last resort as it involves removing the cover from the device. If it is necessary to set Switch 6, refer to your device installation/user's guide for instructions on how to remove the device cover and set Switch 6.

Using FLASH DOWNLOAD CONFIGURATION does not affect the current IP and subnet mask.

Before downloading an image to the device, copy the image to the network TFTP server.

NOTE: For information on how to set up a workstation as a TFTP server, refer to the specific workstation documentation or contact support on the web at:

www.enterasys.com/support/ or refer to Tech Bulletin TK0020-9 (http://www.enterasys.com/support/techtips/tk0020-9.html)

The download and upload configuration capability enables customer configurable settings to be copied from one device to another via the TFTP server, according to the rules described in this section. The configuration file can also be stored on the TFTP server to prevent loosing the configuration values while performing maintenance on the device. After the maintenance is completed, the configuration values can be downloaded to the same device.

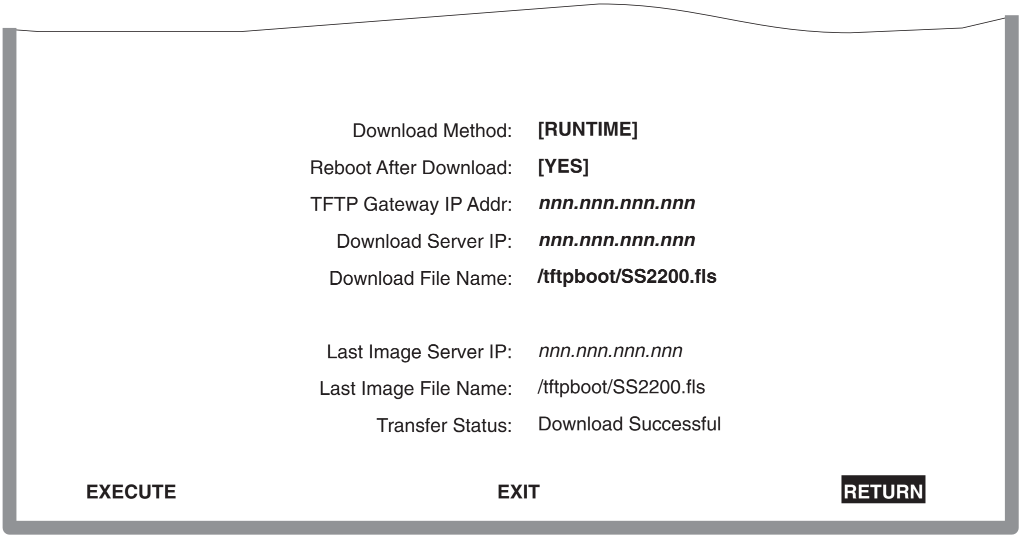
NOTE: Configuration files cannot be downloaded or uploaded directly from one device to another.

How to Access

Use the arrow keys to highlight the **FLASH DOWNLOAD CONFIGURATION** menu item on the Device Configuration Menu screen, and press ENTER. The Flash Download Configuration screen, Figure 4-12, displays.

Screen Example

Figure 4-12 Flash Download Configuration Screen



```
           Download Method:   [RUNTIME]
     Reboot After Download:   [YES]
     TFTP Gateway IP Addr:    nnn.nnn.nnn.nnn
        Download Server IP:   nnn.nnn.nnn.nnn
        Download File Name:   /tftpboot/SS2200.fls

      Last Image Server IP:   nnn.nnn.nnn.nnn
      Last Image File Name:   /tftpboot/SS2200.fls
           Transfer Status:   Download Successful
```

30691_19

Field Descriptions

Refer to Table 4-9 for a functional description of each screen field.

Table 4-9 Flash Download Configuration Screen Field Descriptions

Use this field…	To…
Download Method (Selectable)	Select a method (RUNTIME, DOWNLOAD CONFIG, or UPLOAD CONFIG) to download (receive) an image file from a TFTP server, or upload (transmit) or download a configuration file to/from a TFTP server. The uploading and downloading of a configuration file is accomplished according to the IP address and the file name entered in the Download Server IP and Download File Name fields, respectively. **RUNTIME** – Used to download a new image from a TFTP server. This allows the replacement of the image file currently stored in the device. Section 4.8.1 describes how to download using Runtime. **DOWNLOAD CONFIG** – Used to download a configuration file from a TFTP server to a device. The configuration file must be one that was uploaded to the TFTP server from a device of the same model with the same optional hardware, and running firmware revision 3.10.7 or higher. The device automatically reboots after a successful download. Section 4.8.2 describes how to download a configuration file. **UPLOAD CONFIG** – Used to upload a configuration file from a device to a TFTP server. The configuration file must be one that was downloaded to a device of the same model with the same optional hardware, and running firmware revision 3.10.7 or higher. Section 4.8.3 describes how to download using TFTP.

Table 4-9 Flash Download Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Reboot After Download (Toggle)	Set the device so it will either reboot or not reboot after completing the download of an image. This field toggles between YES and NO, when the Download Method field is set to RUNTIME. If YES is selected, the device reboots after the download is completed. If NO is selected, the device continues using the existing firmware image and stores the new firmware image in FLASH memory. The next time the device is reset or powered-up, the device boots from FLASH memory using the new image. When the Download Method field is set to DOWNLOAD CONFIG, the setting defaults to YES and cannot be changed. In UPLOAD CONFIG, the setting defaults to NO and cannot be changed.
TFTP Gateway IP Addr (Modifiable)	Enter the IP address of the TFTP gateway server defined on the General Configuration screen in Section 4.2.4.
Download Server IP (Modifiable)	Select the IP address of the TFTP server to be used for the download or upload.
Download File Name (Modifiable)	Select the complete TFTP server path and file name of the new image or configuration file.
Last Image Server IP (Read-Only)	See the IP address of the server used for the previous download or upload.
Last Image File Name (Read-Only)	See the complete path and file name of the last downloaded image.
Transfer Status (Read-Only)	See the status of the current or most recent download or upload.

4.8.1 Image File Download Using Runtime

To download a firmware image file to the device using Runtime, proceed as follows:

1. Use the arrow keys to highlight the **Reboot After Download** field.
2. Use the SPACE bar to select either **YES** or **NO**. Select **YES** if you want the device to reboot after the download is completed. Select **NO** if you want the device to store the new image in FLASH memory until the device is reset or during the next power-up.
3. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field.
4. Set the IP address of the TFTP gateway (this defaults to the same IP address as that set in the TFTP Gateway IP Addr field on the General Configuration screen).
5. Use the arrow keys to highlight the **Download Server IP** field.
6. Enter the IP address of the TFTP server using the DDN format.

   For example: *nnn.nnn.nnn.nnn*
7. Use the arrow keys to highlight the **Download File Name** field.
8. Enter the complete pathway and file name of the image stored on the download server.

   For example: /tftpboot/SS2200.fls
9. Use the arrow keys to highlight **EXECUTE** at the bottom of the screen and press ENTER. If Reboot After Download is set to **NO** in step 2, the message “RUNTIME DOWNLOAD IN PROGRESS” displays in the event message line at the top of the screen and the new image is downloaded into FLASH memory. If Reboot After Download is set to **YES** in step 2, the message “REBOOT WILL OCCUR AFTER DOWNLOAD COMPLETES” displays.

   During the downloading process, the screen displays the Download Block Count (the number of frames received).

4.8.2 Configuration File Download Using TFTP

To download a configuration file from a TFTP server to the device, proceed as follows:

1. Use the arrow keys to highlight the **Download Method** field.
2. Use the SPACE bar to select **DOWNLOAD CONFIG**.

NOTE: When DOWNLOAD CONFIG is selected, the Reboot After Download field is automatically set to YES (and cannot be changed), so that the device automatically reboots after a successful download.

3. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field.
4. Set the IP address of the TFTP gateway (this defaults to the same IP address as that set in the **TFTP Gateway IP Addr** field on the General Configuration screen).
5. Use the arrow keys to highlight the **Download Server IP** field.
6. Enter the IP address of the TFTP server using the DDN format.

   For example: *nnn.nnn.nnn.nnn*
7. Use the arrow keys to highlight the **Download File Name** field.
8. Enter the complete pathway and file name of the image stored on the download server.
9. Use the arrow keys to highlight **EXECUTE** at the bottom of the screen and press ENTER. The message "DOWNLOADING CONFIGURATION. REBOOT WILL OCCUR WHEN DOWNLOAD COMPLETES." displays in the event message line at the top of the screen and the configuration file is downloaded to the device from the TFTP server.

4.8.3 Configuration File Upload Using TFTP

To upload a configuration file to a TFTP server, proceed as follows:

1. Use the arrow keys to highlight the **Download Method** field.
2. Use the SPACE bar to select **UPLOAD CONFIG**.

NOTE: When UPLOAD CONFIG is selected, the Reboot After Download field is automatically set to NO (and cannot be changed).

3. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field.
4. Set the IP address of the target TFTP server which is to receive a copy of the device configurable settings.
5. Use the arrow keys to highlight the **Download Server IP** field.
6. Enter the IP address of the target TFTP server using the DDN format.
   For example: *nnn.nnn.nnn.nnn*
7. Use the arrow keys to highlight the **Download File Name** field.
8. Enter the complete pathway and file name of the configuration file in the device.

9. Use the arrow keys to highlight **EXECUTE** at the bottom of the screen and press ENTER. The message **"UPLOAD CONFIGURATION IN PROGRESS"** displays in the event message line at the top of the screen and the device configuration file is uploaded to the TFTP server.

NOTE: The uploading of Passwords can be disabled in the case of sensitive environments. If this capability is enabled, no passwords will be saved to the configuration file.

5

Port Configuration Menu Screens

This chapter describes the Port Configuration Menu screen and the following screens that can be selected:

- Ethernet Interface Configuration screen (Section 5.2)
    - Ethernet Port Configuration screen (Section 5.3)
- HSIM/VHSIM Configuration screen (Section 5.4)
- Redirect Configuration Menu screen (Section 5.5)
    - Port Redirect Configuration screen (Section 5.6)
    - VLAN Redirect Configuration screen (Section 5.7)
- SmartTrunk Configuration screen (Screens are described in the SmartTrunk User’s Guide.)
- Link Aggregation Menu Screen (802.3ad Main Menu Screen) (Section 5.8)
    - Port Screen (Section 5.8.1)
    - Aggregator Screen (Section 5.8.2)
    - System Screen (Section 5.8.3)
- Broadcast Suppression Configuration screen (Section 5.9)

Screen Navigation Path

Password > Device Menu > Device Configuration Menu > **Port Configuration Menu**

5.1 PORT CONFIGURATION MENU SCREEN

When to Use

To select screens to perform port configuration tasks on the switch device.

How to Access

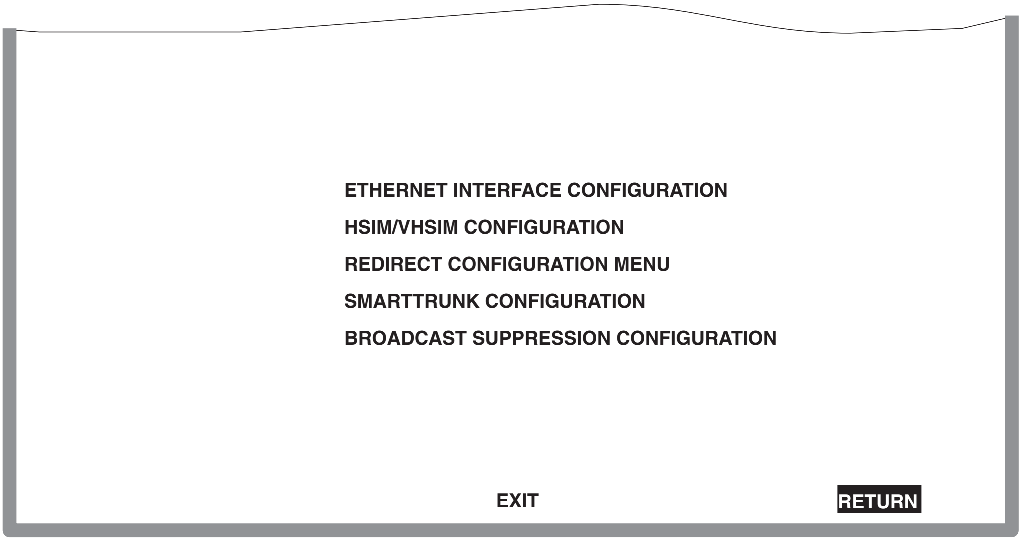
Use the arrow keys to highlight the **PORT CONFIGURATION MENU** item on the Device Configuration Menu screen and press ENTER. The Port Configuration Menu screen, Figure 5-1, displays. The list of menu items is dependent on the Aggregation (Agg) Mode selected in the General Configuration screen described in Section 4.2.

If the Agg Mode “HUNTGROUP” is selected in the General Configuration Menu screen, the Port Configuration Menu screen shown in Figure 5-1, displays.

If the Agg Mode “IEEE8023ad” is selected, the Port Configuration Menu screen shown in Figure 5-2, displays.

Screen Example

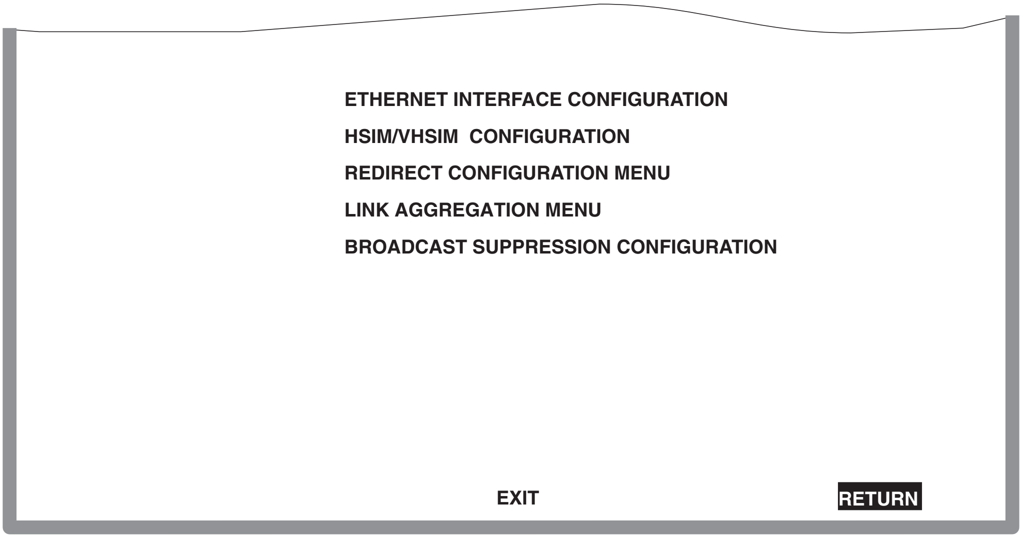
Figure 5-1 Port Configuration Menu Screen (in Agg Mode, HUNTGROUP)



ETHERNET INTERFACE CONFIGURATION
HSIM/VHSIM CONFIGURATION
REDIRECT CONFIGURATION MENU
SMARTTRUNK CONFIGURATION
BROADCAST SUPPRESSION CONFIGURATION

36501_03

Figure 5-2 Port Configuration Menu Screen (in Agg Mode, IEEE8023ad)


ETHERNET INTERFACE CONFIGURATION
HSIM/VHSIM CONFIGURATION
REDIRECT CONFIGURATION MENU
LINK AGGREGATION MENU
BROADCAST SUPPRESSION CONFIGURATION
EXIT
RETURN

3650_13

Menu Descriptions

Refer to Table 5-1 for a functional description of each menu item.

Table 5-1 Port Configuration Menu Screen Menu Item Descriptions

Menu Item	Screen Function
ETHERNET INTERFACE CONFIGURATION	Used to display the link status and current operating mode of each Ethernet port, and provide access to the Ethernet Port Configuration screen, which allows the configuration of the switch device Ethernet ports. For details, refer to Section 5.2.
HSIM/VHSIM CONFIGURATION	Provides access to the HSIM or VHSIM setup screen, depending on the one installed in the device. The screens for optional non-Ethernet HSIMs and VHSIMs are described in their respective user’s guides. For details, refer to Section 5.4.
REDIRECT CONFIGURATION MENU	Provides access to the Port Redirect Configuration and VLAN Redirect Configuration screens. For details, refer to Section 5.5.

Table 5-1 Port Configuration Menu Screen Menu Item Descriptions (Continued)

Menu Item	Screen Function
SMARTTRUNK CONFIGURATION	Used to logically group interfaces together to permit aggregation of multiple links. This menu item appears when the Agg Mode field is set to “HUNTGROUP” in the General Configuration screen. Refer to the *SmartTrunk User’s Guide* for information about how to access and use the SmartTrunk screens.
LINK AGGREGATION MENU	Used to logically group interfaces together to create a greater bandwidth uplink according to the IEEE 802.3ad standard. This menu item appears when the Agg Mode field is set to “IEEE8023ad” in the General Configuration screen. Refer to the Section 5.8 for information about how to access and use the SmartTrunk screens.
BROADCAST SUPPRESSION CONFIGURATION	Used to set a desired limit of received broadcast frames that are forwarded out other interfaces. For details, refer to Section 5.9.

5.2 ETHERNET INTERFACE CONFIGURATION SCREEN

When to Use

To display the link status and current operating mode of each Ethernet port. This screen also provides access to the Ethernet Port Configuration screen, which allows configuration of the Ethernet port.

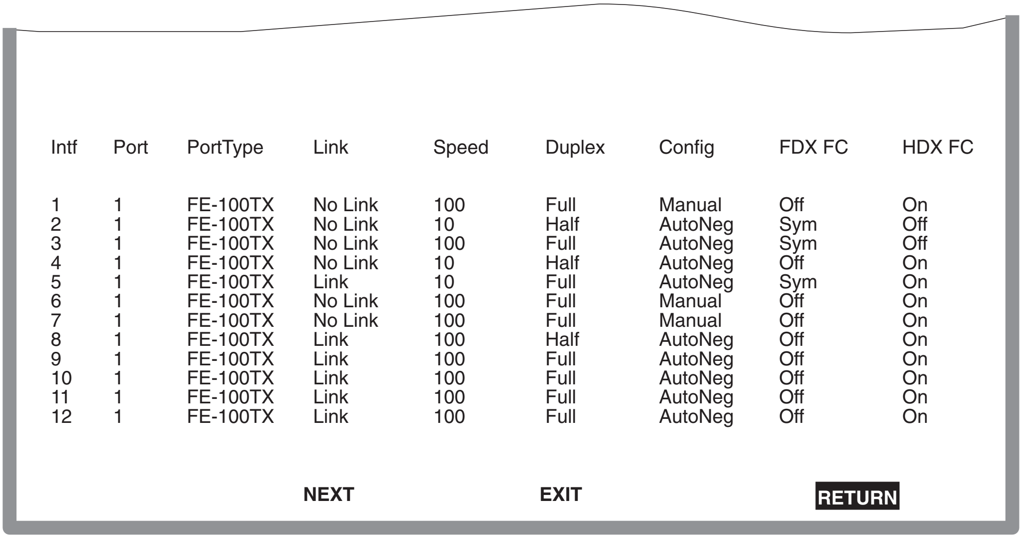
In normal operation, all front panel ports automatically establish a link with the device at the other end of the segment without requiring user setup. However, the Ethernet Interface Configuration screen can be used to access the Ethernet Port Configuration screen to select a port and display its characteristics. The Ethernet Port Configuration screen is used to change the operating mode of the port and enable or disable the advertisement to another device. Refer to Section 5.3 for details.

How to Access

Use the arrow keys to highlight the **ETHERNET INTERFACE CONFIGURATION** menu item on the Port Configuration Menu screen and press ENTER. The Ethernet Interface Configuration screen, Figure 5-3, displays.

Screen Example

Figure 5-3 Ethernet Interface Configuration Screen



```
Intf    Port    PortType    Link       Speed    Duplex    Config     FDX FC    HDX FC

1       1       FE-100TX    No Link    100      Full      Manual     Off       On
2       1       FE-100TX    No Link    10       Half      AutoNeg    Sym       Off
3       1       FE-100TX    No Link    100      Full      AutoNeg    Sym       Off
4       1       FE-100TX    No Link    10       Half      AutoNeg    Off       On
5       1       FE-100TX    Link       10       Full      AutoNeg    Sym       On
6       1       FE-100TX    No Link    100      Full      Manual     Off       On
7       1       FE-100TX    No Link    100      Full      Manual     Off       On
8       1       FE-100TX    Link       100      Half      AutoNeg    Off       On
9       1       FE-100TX    Link       100      Full      AutoNeg    Off       On
10      1       FE-100TX    Link       100      Full      AutoNeg    Off       On
11      1       FE-100TX    Link       100      Full      AutoNeg    Off       On
12      1       FE-100TX    Link       100      Full      AutoNeg    Off       On
```

Field Descriptions

Refer to Table 5-2 for a functional description of each screen field.

Table 5-2 Ethernet Interface Configuration Screen Field Descriptions

Use this field…	To…
Intf (Read-Only)	See the interface number.
Port (Read-Only)	See the number of the physical port on the interface. For the front panel ports on the switch device, this will always be 1.
Port Type (Read-Only)	See the type of interface using the name of the physical port type. For the Ethernet 10/100 Mbps ports in the switch device, FE-100TX will be displayed. If a Fast Ethernet port is installed via an optional HSIM, the interface displayed may be FE-100TX or FE100-FX. If a Gigabit port is installed via an optional VHSIM, the interface displayed may be GE-1000SX, GE-1000LX, or GE-1000CX.

Table 5-2 Ethernet Interface Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Link (Read-Only)	See whether or not there is a physical connection from the port to another device. One of the following values is displayed: Link – There is a link signal present and a valid physical connection to another device. No Link – There is no link signal present and there is no valid physical connection to another device.
Speed (Read-Only)	See the current operational speed in Mbps (10, 100 or 1000). If the port has not completed its auto-negotiation, “NA” displays.
Duplex (Read-Only)	See the current duplex setting as follows: Half – the port is operating in half duplex mode. Full – the port is operating in full duplex mode. NA – the port has not completed its auto-negotiation.
Config (Read-Only)	See whether Auto-Negotiation (AutoNeg) or Manual is enabled. In normal operation, the port with an FE-100TX interface is capable of auto-negotiating the operational mode and no further user setup is required. **NOTE:** In normal operation, the front panel ports of the switch device automatically establish a link with the device at the other end of the segment without requiring user setup. However, Local Management provides the user with the option of manually configuring that port.
FDX FC (Read-Only)	See the current full duplex flow control setting. Flow control is used to manage the transmission between two devices as specified by IEEE 802.3x to prevent receiving ports from being overwhelmed by frames from transmitting devices. One of the following values is displayed: Sym, AsymRx, AsymTx, Off, or NA. NA (Not Applicable) is displayed when the port does not support flow control. Detailed explanations of the other selections are in Section 5.3, under the Full Duplex Flow Control description.

Table 5-2 Ethernet Interface Configuration Screen Field Descriptions (Continued)

Use this field…	To…
HDX FC (Read-Only)	See the current half duplex flow control setting. Half duplex flow control, also known as back pressure, is a collision based flow control mechanism used in half duplex configurations. The port will display On, Off, or NA. NA is displayed when the port does not support flow control.

5.3 ETHERNET PORT CONFIGURATION SCREEN

When to Use

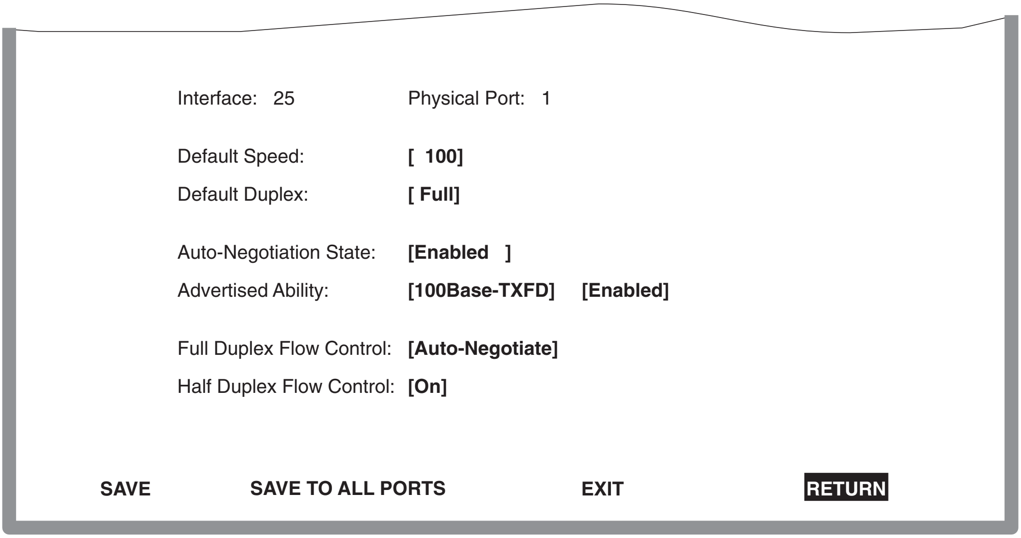
To change the operating mode of a specific Ethernet interface, such as the speed, duplex, auto-negotiation, advertised ability, and the flow control settings. Configuring optional Fast Ethernet or Gigabit Ethernet ports is also done on this screen.

How to Access

Use the arrow keys to highlight the desired Ethernet port from the Ethernet Interface Configuration screen and press ENTER. The Ethernet Port Configuration screen, Figure 5-4, displays for the selected port.

Screen Example

Figure 5-4 Ethernet Port Configuration Screen



```
Interface:   25                 Physical Port:   1

Default Speed:                  [  100]
Default Duplex:                 [ Full]

Auto-Negotiation State:         [Enabled   ]
Advertised Ability:             [100Base-TXFD]    [Enabled]

Full Duplex Flow Control:       [Auto-Negotiate]
Half Duplex Flow Control:       [On]
```

30691_22

Field Descriptions

Refer to Table 5-3 for a functional description of each screen field.

Table 5-3 Ethernet Port Configuration Screen Field Descriptions

Use this field…	To…
Interface (Read-Only)	See the Interface number.
Physical Port (Read-Only)	See the number of the physical port on the interface.
Default Speed (Selectable)	See the current operational speed in Mbps. Display options are **10**, **100**, and **1000**. If Auto-Negotiation is disabled for the port, then the port defaults to operate in the setting displayed. To select a Default Speed, refer to Section 5.3.1.
Default Duplex (Toggle)	Choose the Default Duplex mode: **Half**, for half duplex, or **Full**, for full duplex. If Auto-Negotiation is disabled for the port, then the port defaults to operate in the setting displayed. To choose the Default Duplex, refer to Section 5.3.1.
Auto-Negotiation State (Toggle)	Determine whether Auto-Negotiation is **Enabled** or **Disabled** for the specific port. During auto-negotiation, the port "tells" the device at the other end of the segment what its capabilities are. If Auto-Negotiation is disabled, the port reverts to the speed, duplex and flow control settings specified by Default Speed, Default Duplex, Half Duplex Flow Control and Full Duplex Flow Control fields respectively. To choose the Auto-Negotiation State, refer to Section 5.3.1.

Table 5-3 Ethernet Port Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Advertised Ability (Selectable)	Select the port advertised mode of operation. In normal operation, with all capabilities enabled, the port "advertises" that it has the ability to operate in any mode. The user may choose to set up the port so that only a portion of the available capabilities are advertised and the others are disabled. The left field displays the advertised ability of the port, but only becomes active on ports that have Auto-Negotiation enabled. The status of a particular ability is displayed in the right field. The "T" in an ability stands for twisted pair. The possible abilities are listed below. Only those abilities that are supported will be available. • 10Base-T – 10 Mbps operation • 10Base-TFD – 10 Mbps full duplex operation • 100Base-TX – 100 Mbps operation • 100Base-TXFD – 100 Mbps full duplex operation • 1000Base-X – 1000Base-SX, 1000Base-LX Gigabit Ethernet • 1000Base-T – 1000 Base-T Gigabit Ethernet • 1000Base-XFD – 1000Base-SX, 1000Base-LX Full Duplex Gigabit Ethernet • 1000Base-TFD – 1000Base-T Full Duplex Gigabit Ethernet • FDX PAUSE – Symmetric PAUSE operation for 10/100 Mbps Ethernet ports in full duplex • FDX APAUSE – Asymmetric PAUSE operation for full-duplex links in Gigabit Ethernet • FDX SPAUSE – Symmetric PAUSE operation for full-duplex links in Gigabit Ethernet • FDX BPAUSE – Asymmetric and Symmetric PAUSE operation for full duplex links in Gigabit Ethernet • Rem Fault 1 – simple fault or error detection is supported • Rem Fault 2 – simple fault or error detection is supported • To enable or disable advertised modes, refer to Section 5.3.2.

Table 5-3 Ethernet Port Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Full Duplex Flow Control (Selectable)	Set the flow control feature on each port for a specific mode. The choices are as follows: Symmetric – the port operates in Symmetric mode, causing the port to interpret received PAUSE frames and allow the port to transmit PAUSE frames when necessary at any speed connection. Asymmetric Rx – the port operates in Asymmetric Rx mode, causing the port to interpret received PAUSE frames and prevent the port from transmitting PAUSE frames. This option is for Gigabit only. Asymmetric Tx – the port operates in Asymmetric Tx mode, causing the port to ignore PAUSE frames and allow the port to transmit PAUSE frames when necessary. This option is for Gigabit only. Disabled – full duplex flow control is off, causing the port to ignore received PAUSE frames and prevent the port from transmitting PAUSE frames at any speed connection. Auto-Negotiate – when supported, the maximum flow control capabilities of the port are reflected in the PAUSE bits of the Auto-Negotiation registers. The ports’ flow control operational state is determined by the results of Auto-Negotiation. This option is not displayed if Auto-Negotiation is not supported on this port. To change the settings for full duplex flow control, refer to Section 5.3.1.
Half Duplex Flow Control (Toggle)	Set the Half Duplex flow control mode. Back pressure half duplex flow control is enabled when the port is set **On**, and disabled when the port is set **Off**. To change the settings, refer to Section 5.3.1.
SAVE TO ALL PORTS (Command)	Apply the currently displayed settings on the screen to all ports. To save the settings to all ports, highlight this command and press ENTER.

5.3.1 Selecting Field Settings

All selectable or toggle fields other than Advertised Ability can be changed by following this procedure:

1. Use the arrow keys to highlight the field to be changed.
2. Use the SPACE bar or BACKSPACE key to step or toggle through the selections.
3. Press the ENTER key when the desired selection is displayed.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen. Press ENTER. The selection is saved for that interface. If the setting is to apply to all ports, use the arrow keys to highlight SAVE TO ALL PORTS command and press ENTER. The setting is saved and applied to all ports.

5.3.2 Setting the Advertised Ability

During normal operation, all front panel ports auto-negotiate to the highest speed possible. Under some circumstances, the Network Administrator may want the port to advertise only some of the available modes and not operate in other modes.

To set the advertised ability, proceed as follows:

1. Use the arrow keys to highlight the **Advertised Ability** field.
2. Use the SPACE bar to select the desired mode.
3. Use the arrow keys to move to the **Enabled/Disabled** field.
4. Use the SPACE bar to select **Enabled** or **Disabled**. Press ENTER. If the setting is to apply to all ports, use the arrow keys to highlight the SAVE TO ALL PORTS command and press ENTER. The setting is saved and applied to all ports.
5. Use the arrow keys to move back to the **Advertised Ability** selection and use the SPACE bar to select the next mode to enable or disable.
6. Continue this process until enabling or disabling the advertised modes is completed.
7. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message “SAVED OK” displays and Local Management saves the configuration.

5.4 HSIM/VHSIM CONFIGURATION SCREEN

When to Use

To configure an optional HSIM or VHSIM.

NOTE: The **HSIM/VHSIM Configuration** menu item can only be selected when a non-Ethernet HSIM or VHSIM is installed in the switch device. The applicable setup screen for that interface displays. This only applies to HSIMs and VHSIMs that can support WAN, FDDI or ATM. Refer to the appropriate HSIM or VHSIM user's guide to set its operating parameters.

How to Access

Use the arrow keys to highlight the **HSIM/VHSIM CONFIGURATION** menu item on the Port Configuration Menu screen and press ENTER. The applicable HSIM or VHSIM setup screen displays. Refer to the appropriate HSIM or VHSIM user's guide for instructions on using the Local Management screens for that interface.

5.5 REDIRECT CONFIGURATION MENU SCREEN

Screen Navigation Path

Password > Device Menu > Device Configuration Menu > Port Configuration Menu > **Redirect Configuration Menu**

When to Use

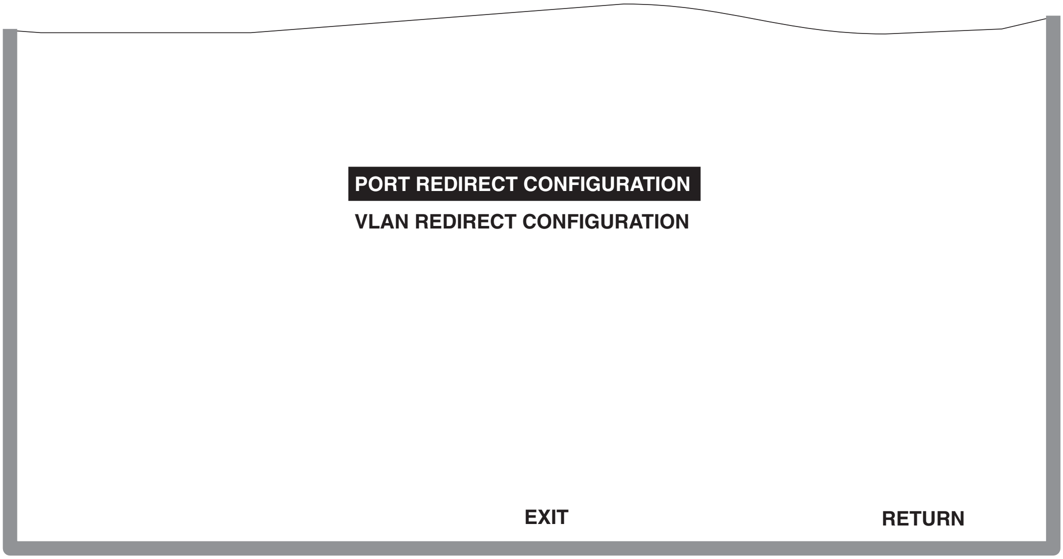
To access the Port Redirect Configuration and VLAN Redirect Configuration screens. Any combination, up to 128, of port and/or VLAN redirect instances can be configured from these screens. This feature is useful in troubleshooting. It enables you to monitor traffic at a destination port using analyzers, RMON probes, and IDS sensors.

How to Access

Use the arrow keys to highlight the **REDIRECT CONFIGURATION MENU** item on the Port Configuration Menu screen and press ENTER. The Redirect Configuration Menu screen, Figure 5-5, displays.

Screen Example

Figure 5-5 Redirect Configuration Menu Screen



30691_23

Menu Descriptions

Refer to Table 5-4 for a functional description of each menu item.

Table 5-4 Redirect Configuration Menu Screen Menu Item Descriptions

Menu Item	Screen Function
PORT REDIRECT CONFIGURATION	Used to redirect traffic in the switch from one source port to many destination ports, or from many source ports to one destination port. For details, refer to Section 5.6.
VLAN REDIRECT CONFIGURATION	Used to direct traffic in the switch of one or more VLANs to one destination port. For details, refer to Section 5.7.

5.6 PORT REDIRECT CONFIGURATION SCREEN

When to Use

To redirect frames in the switch device from one source port to one or more destination ports or from one or more source ports to one destination port. Frames received on the source port can be redirected and transmitted in the frame format in which they are received (normal) or they can be redirected with a VLAN Tag (TAGGED) or without a VLAN Tag (UNTAGGED). Also, any errored frames received can be either dropped or forwarded to the destination port.

For example, port 1 can be set as the source port with ports 2 and 5 as the destination ports. Frames from port 1 are then automatically redirected to ports 2 and 5 according to the configured frame format, and frames with errors can be either forwarded or dropped according to the screen settings.

NOTE: The switch device supports a maximum of 128 redirect entries configured including VLAN redirect, port redirect and, if the module has an optional ATM interface installed, any ATM Permanent Virtual Circuits (PVCs) redirect entries.

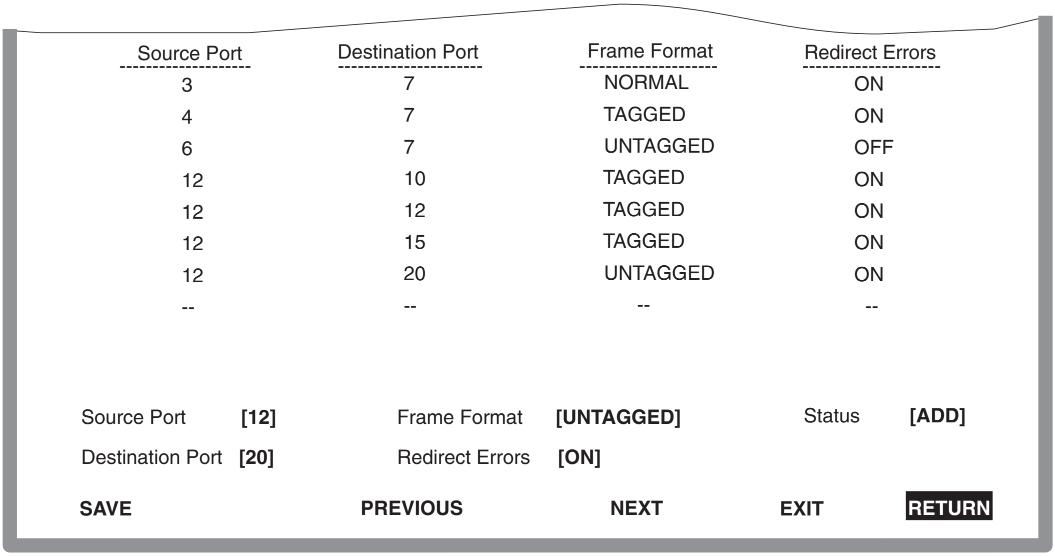
The port redirect function is useful for troubleshooting purposes. It allows all inbound and outbound traffic from one or more source ports to be sent to a destination port where all current traffic from the source ports can be examined using analyzers, RMON probes, or IDS sensors.

NOTE: Although all traffic from the source port (including, if desired, errored frames) is sent to the destination port, normal switching is still performed for all frames on the source port.

How to Access

Use the arrow keys to highlight the **PORT REDIRECT CONFIGURATION** menu item on the Redirect Configuration Menu screen and press ENTER. The Port Redirect Configuration screen, Figure 5-6, displays.

Figure 5-6 Port Redirect Configuration Screen



```
   Source Port        Destination Port       Frame Format          Redirect Errors
 --------------------  ---------------------  --------------------  --------------------
      3                     7                  NORMAL                 ON
      4                     7                  TAGGED                 ON
      6                     7                  UNTAGGED               OFF
      12                    10                 TAGGED                 ON
      12                    12                 TAGGED                 ON
      12                    15                 TAGGED                 ON
      12                    20                 UNTAGGED               ON
      --                    --                 --                     --


 Source Port       [12]        Frame Format      [UNTAGGED]       Status     [ADD]

 Destination Port  [20]        Redirect Errors   [ON]
```

3528-22

Field Descriptions

Refer to Table 5-5 for a functional description of each screen field.

Table 5-5 Port Redirect Configuration Screen Field Descriptions

Use this field…	To…
Source Port (Read-Only)	See the VLAN ID of the VLANs that are currently set as source VLANs. (Multiple VLANs may be assigned to one destination port.)
Destination Port (Read-Only)	See which ports are currently set as destination ports. There can be only one destination port associated with one or more VLANs.

Table 5-5 Port Redirect Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Frame Format (Read-Only)	See the current frame format setting: NORMAL, TAGGED, or UNTAGGED. The default is NORMAL. NORMAL – Frames are redirected in the format that they were received or transmitted on the source port. TAGGED – Frames are transmitted on the destination port with a VLAN tag inserted according to the frame classification. UNTAGGED – Frames are transmitted on the destination port without a VLAN tag regardless of the format of the received frame.
Redirect Errors (Read-Only)	See whether the corresponding source ports are configured ON to send errored frames to the destination ports, or OFF to drop all errored frames and only forward valid frames to the destination ports. All redirected error frames display in the way they were received or transmitted on the source port, regardless of the frame format setting.
Source Port [*n*] (Selectable)	Select the port [*n*] that is to be changed to a source port. For details, refer to Section 5.6.1.
Destination Port [*n*] (Selectable)	Select the port [*n*] that is to be changed to a destination port. For details, refer to Section 5.6.1.
Frame Format (Selectable)	Select the frame format for the transmission of redirected frames on the destination port. NORMAL, TAGGED, or UNTAGGED may be selected. Refer to the previously described read-only Frame Format field for details about each format. The default setting is NORMAL.
Redirect Errors (Toggle)	Set each source port to either ON, to send errored frames to its destination port, or OFF to drop errored frames and send only valid traffic to its destination port. The default setting is OFF.
Status (Toggle)	Add or delete source and destination ports selected in the Source Port [*n*] and Destination Port [*n*] fields.

5.6.1 Changing Source and Destination Ports

To add or delete source port and destination port entries and set the Frame Format and Redirect Errors functions, proceed as follows:

1. Use the arrow keys to highlight the **Source Port** field near the bottom of the screen.
2. Press the SPACE bar or BACKSPACE key one or more times to increment or decrement the port number displayed in the brackets [*n*] until the appropriate port number displays.
3. Use the arrow keys to highlight the **Destination Port** field near the bottom of the screen.
4. Use the SPACE bar or BACKSPACE key to step to the appropriate port number for the destination port.
5. Use the arrow keys to highlight the **Frame Format** field near the bottom of the screen.
6. Use the SPACE bar or BACKSPACE key to step to the appropriate frame format setting (**NORMAL**, **TAGGED**, or **UNTAGGED**) for the selected Destination Port.
7. Use the arrow keys to highlight the **Redirect Errors** field near the bottom of the screen.
8. Use the SPACE bar to select either the **ON** or **OFF** option and press ENTER. The **ON** selection forces the source port to forward errored frames to the destination port(s). **OFF** forces the errored frames to be dropped before forwarding traffic.
9. Use the arrow keys to highlight the **Status** field.
10. Use the SPACE bar to select either the **ADD** or **DEL** (delete) option. Press ENTER. This adds or deletes the selections for the Source Port, Destination Port, Frame Format, and Redirect Errors made in steps 1 through 8 and also updates the screen.

TIP: If more than 1 port is being redirected, repeat steps 1 through 10 for each additional setting. Then go to step 11 to save all the new settings at once.

If an entry is to be changed, delete the entry, save the screen, then recreate the entry with its new settings.

NOTE: Any combination, up to 128, of port redirect instances (configured on the Port Redirect Configuration screen) and/or VLAN redirect instances (configured on the VLAN Redirect Configuration screen) can be configured.

11. Use the arrow keys to highlight **SAVE** at the bottom of the screen. Press ENTER. The message "SAVED OK" displays. This saves the new settings and updates the Source Port and Destination Port read-only fields.

5.7 VLAN REDIRECT CONFIGURATION SCREEN

When to Use

To select a source VLAN ID and a destination port. For example, VLAN ID 1 can be set as the source VLAN with port 2 as the destination port. Traffic from VLAN ID 1 is then automatically redirected to port 2 according to the Frame Format setting for that source VLAN. The Frame Format setting determines the format in which the frames received belonging to the source VLAN are redirected to the destination port. The frames can be forwarded in the frame format as received, tagged, or untagged.

The VLAN redirect function is useful for troubleshooting purposes, as it allows traffic associated with a particular VLAN to be sent to a particular port where, with the use of an analyzer or RMON probe, all current traffic from the source VLAN can be examined.

NOTE: Although traffic associated with a particular VLAN is sent to the destination port, normal switching is still performed for all frames on the source port.

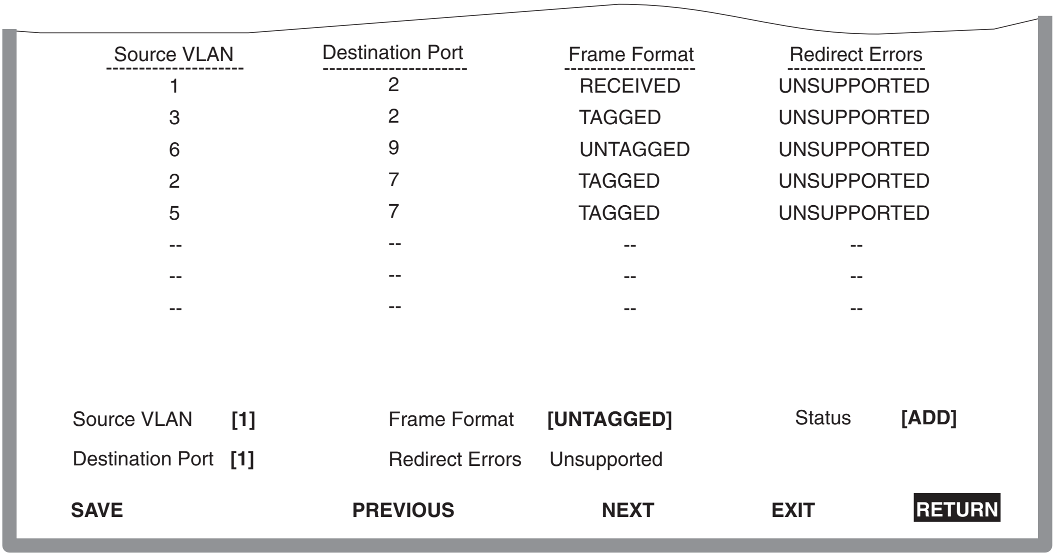
The Redirect Errors function is not supported on this screen.

How to Access

Use the arrow keys to highlight the **VLAN REDIRECT CONFIGURATION** menu item on the Redirect Configuration Menu screen and press ENTER. The VLAN Redirect Configuration screen, Figure 5-7, displays.

Screen Example

Figure 5-7 VLAN Redirect Configuration Screen



```
  Source VLAN        Destination Port      Frame Format       Redirect Errors
---------------    -------------------   ----------------    -----------------
       1                   2               RECEIVED           UNSUPPORTED
       3                   2               TAGGED             UNSUPPORTED
       6                   9               UNTAGGED           UNSUPPORTED
       2                   7               TAGGED             UNSUPPORTED
       5                   7               TAGGED             UNSUPPORTED
       --                  --                 --                  --
       --                  --                 --                  --
       --                  --                 --                  --


Source VLAN        [1]         Frame Format     [UNTAGGED]        Status     [ADD]

Destination Port   [1]         Redirect Errors  Unsupported
```

Field Descriptions

Refer to Table 5-6 for a functional description of each screen field.

Table 5-6 VLAN Redirect Configuration Screen Field Descriptions

Use this field…	To…
Source VLAN (Read-Only)	See the VLAN ID of the VLANs that are currently set as source VLANs.
Destination Port (Read-Only)	See which ports are currently set as destination ports. (Multiple VLANs may be assigned to a destination port.)
Frame Format (Read-Only)	See the current frame format setting: RECEIVED, TAGGED, or UNTAGGED. The default is RECEIVED. • RECEIVED – Frames are redirected in the format that they were received by the switch device. • TAGGED – Frames are transmitted on the destination port with a VLAN tag inserted according to the frame classification of the receiving port. • UNTAGGED – Frames are transmitted on the destination port without a VLAN tag regardless of the format of the received frame.
Redirect Errors	Unsupported.
Source VLAN [*n*] (Modifiable)	Enter the VLAN ID of the VLAN that is to be changed to a source VLAN. For details, refer to Section 5.7.1.
Destination Port [*n*] (Selectable)	Select the port number that is to be changed to a destination port. For details, refer to Section 5.7.1.
Frame Format (Selectable)	Select the frame format for the transmission of redirected frames on the destination port. RECEIVED, TAGGED, or UNTAGGED may be selected. Refer to the previously described read-only Frame Format field for details about each format. The default setting is RECEIVED.
Redirect Errors	Unsupported.
Status (Toggle)	Add or delete source and destination ports selected in the Source VLAN [*n*] and Destination Port [*n*] fields.

5.7.1 Changing Source VLAN and Destination Ports

To add or delete source VLAN and destination port entries and set the Frame Format, proceed as follows:

1. Use the arrow keys to highlight the **Source VLAN** field near the bottom of the screen.
2. Type in the VLAN ID number of the source VLAN to be configured.
3. Use the arrow keys to highlight the **Destination Port** field near the bottom of the screen.
4. Use the SPACE bar or BACKSPACE key to step to the appropriate port number for the destination port.
5. Use the arrow keys to highlight the **Frame Format** field near the bottom of the screen.
6. Use the SPACE bar or BACKSPACE key to step to the appropriate frame format setting (**RECEIVED**, **TAGGED**, or **UNTAGGED**) for the selected Destination Port.
7. Use the arrow keys to highlight the **Status** field.
8. Use the SPACE bar to select either the **ADD** or **DEL** (delete) option. Press ENTER. This adds or deletes the selections for the Source VLAN, Destination Port, and Frame Format made in steps 1 through 6 and also updates the screen.

TIP: If more than 1 port is being redirected, repeat steps 1 through 8 for each additional setting. Then go to step 9 to save all the new settings at once.

If an entry is to be changed, delete the entry, save the screen, then recreate the entry with its new settings.

Any combination, up to 128, of port redirect instances (configured on the Port Redirect Configuration screen) and/or VLAN redirect instances (configured on the VLAN Redirect Configuration screen) can be configured.

9. Use the arrow keys to highlight **SAVE** at the bottom of the screen. Press ENTER. The message “SAVED OK” displays. This saves the new settings and updates the Source Port and Destination Port read-only fields.

5.8 LINK AGGREGATION MENU SCREEN (802.3ad MAIN MENU SCREEN)

Screen Navigation Path

Password > Device Menu > Device Configuration Menu > Port Configuration Menu > **Link Aggregation Menu**

CAUTION: These screens should be used only by personnel who are knowledgeable about Spanning Tree and Link Aggregation and fully understand the ramifications of modifications beyond defaults. Otherwise, the proper operation of the network could be at risk.

When to Use

To access the Port, Aggregator, or System information screens, and to configure port trunking according to the IEEE 802.3ad standard.

Usage Notes

In normal usage (and typical implementations) there is no need to modify any of these parameters. The default values will result in the maximum number of aggregation possible. If the switch is placed in a configuration with its peers not running the protocol, no aggregations will be formed and the switch will function normally (that is, will block redundant paths).

IEEE 802.3ad determines if ports are physically capable of aggregating by comparing the operational keys of ports.With this IEEE 802.3ad implementation, the operation key is the same as the administrative key assigned by management, so ports assigned different administrative key values will then have different operational key values, and will not aggregate.

Aggregators also have an administrative and operational key. If a group of ports are in the same LAG (Link Aggregation Group) but there is no aggregator with a matching operational key, they will not be able to aggregate.

IEEE 802.3ad allows groups of ports to be considered as being in different systems within the same switch. The system priority is used in conjunction with the System Identifier to determine the switch’s system ID. Similarly to Keys, if ports are given different system priority values they will not aggregate. In addition, this system priority has to match the system priority of an aggregator or no connection can be made.

According to the IEEE 802.3ad standard, a port does not detach from an aggregator because of link loss. If a port is attached to an aggregator and the link is removed, the port’s mux machine will transition from COLLECTING to ATTACHED; however, it will remain attached to the same aggregator.

Ports that are attached to an aggregator will enter a Spanning Tree state of AGGREGATING on the Spanning tree screens, just as they do when manually placed in a trunk.

In this implementation, the concept of an aggregator is for a non-aggregated port to attach to, although this aggregator doesn't exist in any real sense. A port that is not a member of an aggregation will be displayed in LM as attached to a non-existent aggregation. If a port instance matches the aggregator instance it is attached to, that means it is not aggregating.

There are a few cases in which the 802.3ad implementation will disable a port's ability to aggregate by clearing the aggregable bit ActorOperState:

- A port is attached to another port on this same switch (loopback). There is no available aggregator for 2 or more ports with the same LAGID. This can happen if either there are simply no available aggregators, or if none of the aggregators have a matching operational key and system priority.
- A port is in the same LAG as another port but is running at a slower speed. Ports running at different speeds are not allowed to aggregate according to 802.3ad.

NOTE: Ports running at half-duplex cannot aggregate.

There is a maximum of six aggregators per module.

Definitions to Know

Rapid Reconfiguration Spanning Tree

Rapid Reconfiguration is an enhancement to the legacy 802.1D Spanning Tree implementation, which implements a rapidly converging Spanning Tree algorithm that is event-driven instead of timer-driven.

Spanning Tree

When multiple links are connected from one switch to another, it is necessary that only one link be allowed to switch network traffic. Due to the functionality of a switch, if multiple links were active, a packet would end up “looping” around in those links indefinitely. This problem is well documented and is the reason that bridges implement the Spanning Tree Protocol (STP).

The STP is able to calculate which ports on a switch can be allowed to forward traffic to eliminate the possibility of looping in a network. So, if multiple links were attached between two switches, only one would be used. The remaining links would be placed in a disabled state called “Blocking.”

Link Aggregation

It is desirable to have a way to use multiple interswitch links simultaneously to increase interswitch bandwidth. This can be done if both sides agree on a set of ports that are being used as an interswitch link called a “Trunk.” As long as both switches agree on which ports are in this trunk, there are no problems with looping, and the Spanning Tree can treat this trunk as a single port.

Proprietary Aggregation Methods

Most switch vendors provide a way to group these ports together manually. For example, the user could configure Ports 1, 2 and 3 in a trunk on switch X and connect to ports 4, 5 and 6 that are in a trunk on switch Y. By interconnecting the switches together, the effective bandwidth can be aggregated to the sum of the parts. The Enterasys Networks’ implementation is called SmartTrunking.

IEEE 802.3ad

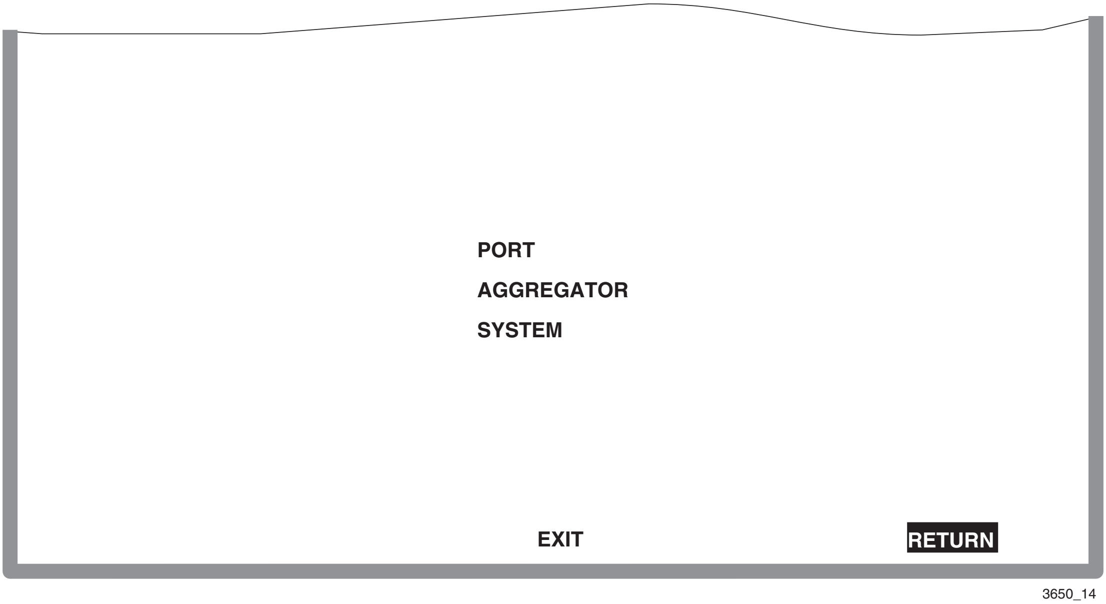
All the methods of trunking multiple links have involved manually choosing the links that are part of the trunk. The IEEE 802.3ad specification allows the switch to determine which links are in trunks and configure them dynamically. Since the protocol is based on IEEE standards specifications, any switch from any vendor that supports this protocol can trunk links automatically.

How to Access

Use the arrow keys to highlight the **LINK AGGREGATION MENU** item in the Port Configuration Menu screen described in Section 5.1 and press ENTER. The 802.3ad MAIN MENU screen, Figure 5-8, displays.

Screen Example

Figure 5-8 802.3ad Main Menu Screen



Menu Descriptions

Refer to Table 5-7 for a functional description of each menu item.

Table 5-7 802.3ad Main Menu Screen Menu Item Descriptions

Menu Item	Screen Function
PORT	Used to access the 802.3ad Port screen, described in Section 5.8.1, to view port instances and to access the 802.3ad Port Details screen, described in Section 5.8.1.1, and the port Statistics screen, described in Section 5.8.1.2.
AGGREGATOR	Used to access the 802.3ad Aggregator screen to display a summary of all the available aggregators and a other basic information, including the aggregator interface instance, operational key, system priority, and the number of ports currently attached to the aggregator. For details about the 802.3ad Aggregator screen, refer to Section 5.8.2. The 802.3ad Aggregator screen also enables you to access the 802.3ad Aggregator Details screen for a particular port instance to modify, or view its Aggregator parameters as described in Section 5.8.2.1.
SYSTEM	Used to view the 802.3ad System screen to see basic system-level information: System Identifier, Number of Ports, and Number of Aggregators. For details, refer to Section 5.8.3.

5.8.1 802.3ad Port Screen

When to Use

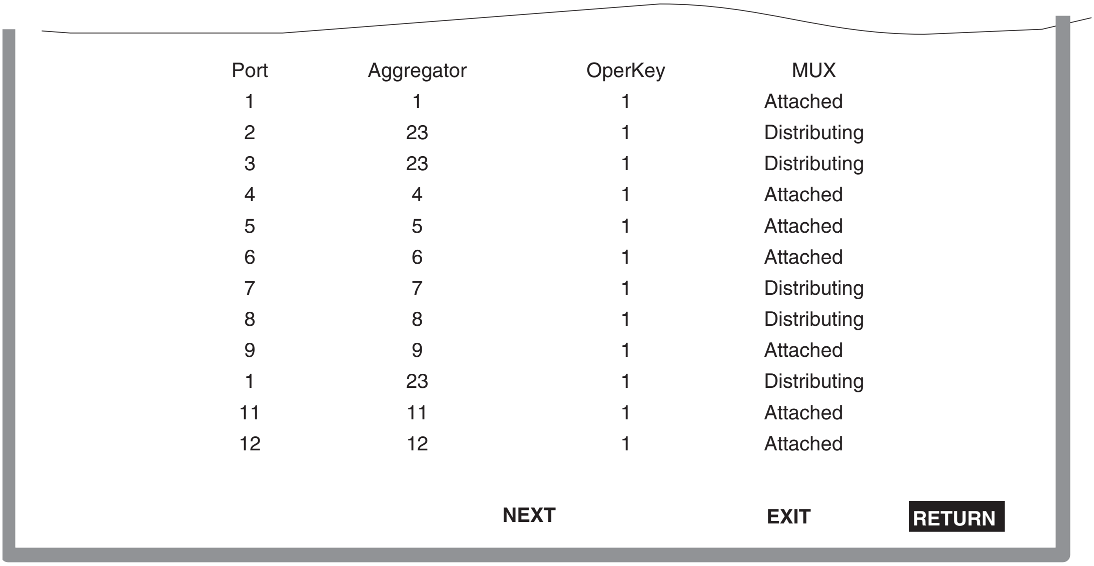
To display a summary of all the ports that are running 802.3ad and the information concerning the ports associated with each Aggregator, the Operational Key, and the state of the port’s MUX state machine.

How to Access

Use the arrow keys to highlight the **PORT** menu item in the Link Aggregation Menu (802.3ad Main Menu) screen, described in Section 5.8, and press ENTER. The 802.3ad Port screen, Figure 5-9, displays.

Screen Example

Figure 5-9 802.3ad Port Screen



Port	Aggregator	OperKey	MUX
1	1	1	Attached
2	23	1	Distributing
3	23	1	Distributing
4	4	1	Attached
5	5	1	Attached
6	6	1	Attached
7	7	1	Distributing
8	8	1	Distributing
9	9	1	Attached
1	23	1	Distributing
11	11	1	Attached
12	12	1	Attached

3650_15

Field Descriptions

Refer to Table 5-8 for a functional description of each screen field.

Table 5-8 802.3ad Port Screen Field Descriptions

Use this field…	To…
Port (Read-Only)	View the port number, which correlates to the port numbers in other screens.
Aggregator (Read-Only)	View the instance of the aggregator and the attached port. If the aggregator instance matches the port instance then the port is not aggregating with any other port.
OperKey (Read-Only)	View operation key of the port. For ports to aggregate they must have the same operation key.
MUX (Read-Only)	View the state of the port's mux state machine. It can have values of DETACHED, ATTACHED, WAITING, COLLECTING or DISTRIBUTING. If a port is connected to another port, this field would display DISTRIBUTING. Otherwise, ATTACHED is displayed.

Figure 5-9 shows the four columns of information: The Port Instance; the Aggregator that the Port is attached to; the operational key of the Port, and the state of the port's MUX state machine.

Viewing and Editing 802.3ad Port Parameters

To view the 802.3ad related port parameters of any port displayed on the screen, proceed as follows:

1. Use the arrow keys to highlight the port number of interest under the **Port** field.
2. Press ENTER. The 802.3ad Port Details screen described in Section 5.8.1.1 is displayed. Once in this screen, the parameters of any selected 802.3ad port can be edited and saved.

5.8.1.1 802.3ad Port Details Screen

When to Use

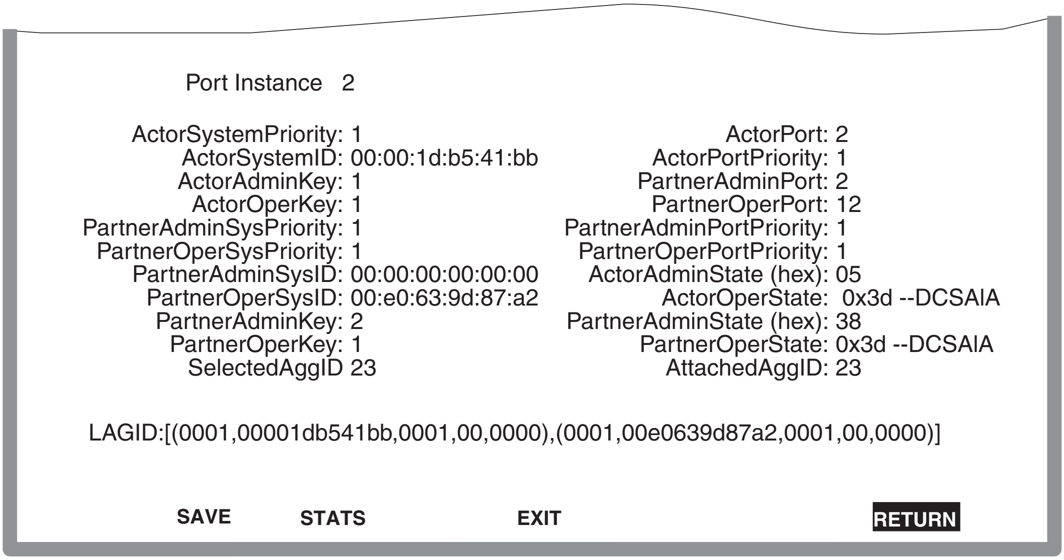
To view and configure all the port-related LACP parameters of any port instance shown in the 802.3ad Port screen described back in Section 5.8.1.

How to Access

Use the arrow keys to highlight the line with the port of interest to display the details about that port and press ENTER. The 802.3ad Port Details screen, Figure 5-10, is displayed, showing the details of the port parameters (in this example for Port Instance 2) that can be modified.

Screen Example

Figure 5-10 802.3ad Port Details Screen



```
                 Port Instance   2

      ActorSystemPriority: 1                           ActorPort: 2
            ActorSystemID: 00:00:1d:b5:41:bb   ActorPortPriority: 1
           ActorAdminKey: 1                      PartnerAdminPort: 2
             ActorOperKey: 1                      PartnerOperPort: 12
 PartnerAdminSysPriority: 1              PartnerAdminPortPriority: 1
  PartnerOperSysPriority: 1               PartnerOperPortPriority: 1
      PartnerAdminSysID: 00:00:00:00:00:00  ActorAdminState (hex): 05
       PartnerOperSysID: 00:e0:63:9d:87:a2       ActorOperState:  0x3d --DCSAIA
          PartnerAdminKey: 2              PartnerAdminState (hex): 38
           PartnerOperKey: 1                   PartnerOperState: 0x3d --DCSAIA
            SelectedAggID 23                      AttachedAggID: 23

   LAGID:[(0001,00001db541bb,0001,00,0000),(0001,00e0639d87a2,0001,00,0000)]
```

3650-011_16

Field Descriptions

Refer to Table 5-9 for a functional description of each screen field.

Table 5-9 802.3ad Port Details Screen Field Descriptions

Use this field…	To…
Port Instance (Read-Only)	See the port number, which correlates to the port numbers in other screens.
ActorSystemPriority (Modifiable)	Set the system priority associated with this port for use used in the construction of the LAG ID of the port.
ActorPort (Read-Only)	See the identifier for this port (identical to Port Instance).
ActorSystemID (Read-Only)	See the System Identifier for the system in which this port resides.
ActorPortPriority (Modifiable)	Set the priority value of this port (not used in this implementation).
ActorAdminKey (Read-Only)	See the administratively assigned key value for this port. Only ports with matching keys may aggregate.
PartnerAdminPort (Modifiable)	Enter a default value for PartnerOperPort when no protocol partner is available.
ActorOperKey (Read-Only)	See the current operation key for this port. Only ports with matching operation keys may aggregate.
PartnerOperPort (Read-Only)	See ActorPort on the partner switch that we are currently attached to.
PartnerAdminSysPriority (Modifiable)	Set a default value to use for the PartnerOperSysPriority when no protocol partner is available.
PartnerAdminPortPriority (Modifiable)	Set a default value to use for the PartnerOperPortPriority when no protocol partner is available.
PartnerOperSysPriority (Read-Only)	See the system priority of the partner port used to construct this port's LAGID.
PartnerOperPortPriority (Read-Only)	See the port priority of the partner port (not used in this implementation).

Table 5-9 802.3ad Port Details Screen Field Descriptions (Continued)

Use this field…	To…
PartnerAdminSysID (Modifiable)	Set a default value to use for PartnerAdminSysID when no protocol partner is available.
ActorAdminState (hex) (Modifiable)	Set the administrative value for this port’s Actor_State. Allows administrative control over the values of LACP_Activity, LACP_Timeout and Aggregation.
PartnerOperSysID (Read-Only)	See system ID of this port’s partner.

Table 5-9 802.3ad Port Details Screen Field Descriptions (Continued)

Use this field…	To…
ActorOperState (Read-Only)	The current (operational) value of the port’s Actor_State. The hex value is displayed as well as the individual bit fields. The fields are as follows. bit 0 LACP_Activity, 1 indicates **A**ctive, 0 indicates **p**assive. If a port is Active, it will always transmit LACP PDUs. If it is passive, it will only transmit LACP PDUs if it sees LACP PDUs coming from its partner. If the bit is set, an ‘A’ is displayed, otherwise a ‘p’ is displayed. bit 1 LACP_Timeout, 1 indicates **S**hort timeout, 0 indicates **l**ong timeout. A Short timeout indicates that this port will time out information if an LACP PDU is not received for 3 seconds, a long timeout indicates that this port will time out information if an LACP PDU is not received for 90 seconds. If this bit is set, an ‘S’ is displayed, otherwise, an ‘l’ is displayed. bit 2 Aggregation, 1 indicates that a port is **A**ggregable, 0 indicates that a port is **i**ndividual. If a port is capable of being aggregated with other ports then this bit will be 1, otherwise this port will be 0. If this bit is 1 an ‘A’ is displayed, otherwise an ‘i’ is displayed. bit 3 Synchronization, 1 indicates we are **S**yncronized, 0 indicates that we are not synchronized. If a port has selected and attached to the correct aggregator then a port is said to be synchronized. If this bit is true an ‘S’ is displayed, otherwise a ‘-’ is displayed for this bit position. bit 4 Collecting, 1 indicates we are **C**ollecting, 0 indicates that this port is not collection. “Collecting” means that a port is ready to receive traffic. If Collecting is true a ‘C’ is displayed, otherwise, a ‘-’ is displayed in this bit position.

Table 5-9 802.3ad Port Details Screen Field Descriptions (Continued)

Use this field…	To…
ActorOperState (Read-Only) **(Continued)**	bit 5 Distributing, 1 indicates that we are **D**istributing. “Distributing” means that a port is ready to transmit traffic. If Distributing is true a ‘D’ is displayed, otherwise a ‘-’ is displayed in this bit position. bit 6 Defaulted, 1 indicates that we have de**F**aulted. If no protocol partner is available a port will resort to using default information about its partner. When this happens a port is said to be defaulted. If this bit is 1 an ‘F’ is displayed, otherwise a ‘-’ is displayed in this bit position. bit 7 Expired, 1 indicates that we have **E**xpired. This indicates that no LACP PDUs have been received for a sufficient length of time so the partner information has expired. If this is true, an ‘E’ is displayed, otherwise a ‘-’ is displayed in this bit position.
PartnerAdminKey (Modifiable)	Set a default value to use for PartnerOperKey when no protocol partner is available.
PartnerAdminState (hex) (Modifiable)	Set a default value to use for PartnerOperState when no protocol partner is available.
PartnerOperKey (Read-Only)	See a default value to use for PartnerOperState when no protocol partner is available.
PartnerOperState (Read-Only)	See current state value of the partner port (same bits as the ActorOperState).
SelectedAggID (Read-Only)	See the instance of the aggregator that this port has selected.
AttachedAggID (Read-Only)	See the instance of the aggregator to which this port is attached.

Table 5-9 802.3ad Port Details Screen Field Descriptions (Continued)

Use this field…	To…
LAGID (Read-Only)	See the complete link aggregation group identifier for the port. Ports with identical LAGIDs will be connected to the same aggregator. The various PartnerAdmin values are copied into the corresponding PartnerOper fields when no protocol partner is present (see RecordDefault in the AD spec). This allows for manual configuration of groups when no protocol partner is present.
STATS (Command)	Open the 802.3ad Port Statistics screen described in Section 5.8.1.2 to display the current statistics of the port displayed in the Port Instance field.

Viewing and Editing 802.3ad Port Parameters

To change a parameter, proceed as follows:

1. Use the arrow keys to highlight the parameter field to be modified and type in the new value. Press ENTER. Repeat this step to change other parameter settings as necessary before saving the new settings.
2. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
3. Press ENTER. The message “SAVED OK” displays. All settings are saved.

Displaying Port Statistics

To display statistical information about the port displayed in the Port Instance field, proceed as follows:

1. Use the arrow keys to highlight the **STATS** command at the bottom of the screen.
2. Press ENTER. The 802.3ad Port Statistics screen described in Section 5.8.1.2 is displayed, showing the current port statistics.

5.8.1.2 802.3ad Port Statistics Screen

When to Use

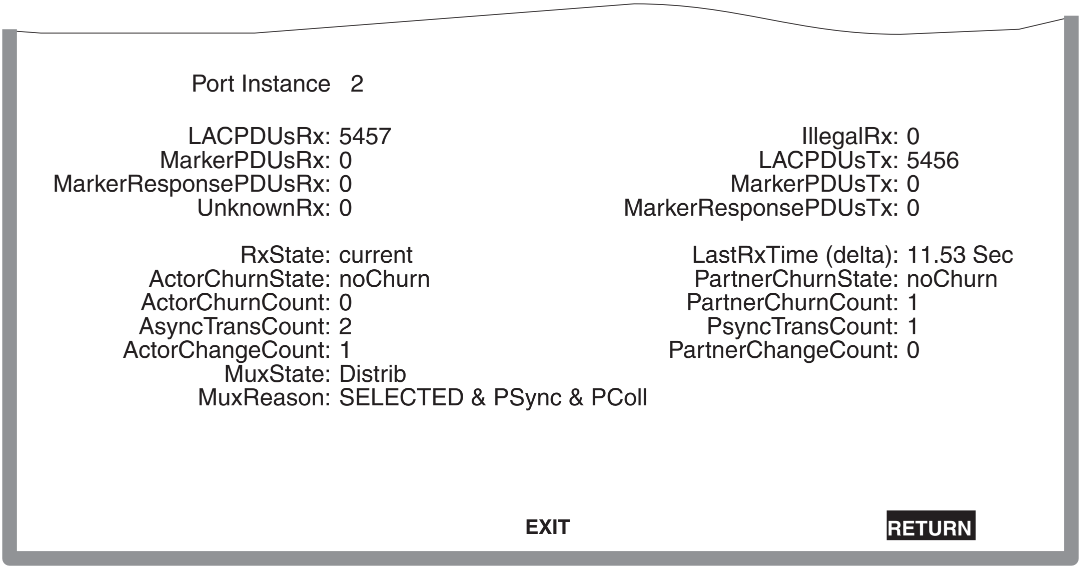
To view all the port-related LACP parameters about a port instance shown in the 802.3ad Port Details screen described back in Section 5.8.1.1.

How to Access

Use the arrow keys to highlight the **STATS** command in the 802.3ad Port Details screen and press ENTER. The 802.3ad Port Statistics screen (Figure 5-11) displays. The figure shows an example of how the details are displayed (in this example for Port Instance 2).

Screen Example

Figure 5-11 802.3ad Port Statistics Screen



```
                  Port Instance   2

                LACPDUsRx: 5457                                     IllegalRx: 0
           MarkerPDUsRx: 0                                         LACPDUsTx: 5456
MarkerResponsePDUsRx: 0                                        MarkerPDUsTx: 0
              UnknownRx: 0                        MarkerResponsePDUsTx: 0

                   RxState: current                          LastRxTime (delta): 11.53 Sec
       ActorChurnState: noChurn                         PartnerChurnState: noChurn
       ActorChurnCount: 0                                PartnerChurnCount: 1
       AsyncTransCount: 2                                   PsyncTransCount: 1
   ActorChangeCount: 1                               PartnerChangeCount: 0
                  MuxState: Distrib
              MuxReason: SELECTED & PSync & PColl
```

3650-011_17

Field Descriptions

Refer to Table 5-10 for a functional description of each screen field.

Table 5-10 802.3ad Port Statistics Screen Field Descriptions

Use this field…	To…
Port Instance (Read-Only)	See a unique number used to identify this port. This corresponds to the port numbering scheme seen in other screens.
LACPDUsRx (Read-Only)	See the number of valid Marker PDUs that this Aggregation Port can receive.
IllegalRx (Read-Only)	See the number of received frames carrying the Slow Protocol's Ethernet Type value (34B.4), and also contain a badly formed PDU or a value of Protocol Subtype (43B.4) that is illegal.
MarkerPDUsRx (Read-Only)	See the number of valid Marker Response PDUs that this Aggregation Port can receive.
LACPDUsTx (Read-Only)	See the number of LAC PDUs that this Aggregation Port can transmit.
MarkerResponsePDUsRx (Read-Only)	See the number of Marker Response PDUs that this Aggregation Port can transmit.
MarkerPDUsTx (Read-Only)	See the number of Marker PDUs that this Aggregation Port can transmit.
UnknownR (Read-Only)	See the number of Unknown frames that can be received that either • carry the Slow Protocols Ethernet Type value but contain an unknown PDU, or • are addressed to the Slow Protocols group MAC Address but do not carry the Slow Protocols Ethernet Type. This is a 32-bit counter of the number of Unknown frames received, so the value can range from 0 to 2^32-1 (or 0 to 4,294,967,296) frames.
MarkerResponsePDUsTx **(**Read-Only)	See the number of Marker Response PDUs that this Aggregation Port can transmit.
RxState (Read-Only)	See the state of the Receive state machine for this port.

Table 5-10 802.3ad Port Statistics Screen Field Descriptions (Continued)

Use this field…	To…
LastRxTime(delta) (Read-Only)	See the amount of time since the last LACP PDU has been received on this port.
ActorChurnState (Read-Only)	See the state of the Actor Churn state machine for this port. Values can be noChurn, churn, or churnMonitor. Churn indicates that the port is unable to find an aggregator to attach to.
PartnerChurnState (Read-Only)	See the state of the Partner Churn state machine for this port.
ActorChurnCount (Read-Only)	See the number of times this port’s Actor Churn machine has entered the churn state.
PartnerChurnCount (Read-Only)	See the number of times this port’s Partner Churn machine has entered the churn state.
AsyncTransCount (Read-Only)	See a count of how many times the Actor’s Mux state machine enters the IN-Sync state.
PsyncTransCount (Read-Only)	See a count of how many times the Partner’s Mux state machine enters the IN-Sync state.
ActorChangeCount (Read-Only)	See a count of how many times the Actor’s perception of the LAG ID changes for this Aggregation Port.
PartnerChangeCount (Read-Only)	See a count of how many times the Partner’s perception of the LAG ID (see 43.3.6.1) changes for this Aggregation Port.
MuxState (Read-Only)	See the state of the Mux state machine for this port.
MuxReason (Read-Only)	See the string of text describing why the Mux machine is in its current state.

5.8.2 802.3ad Aggregator Screen

When to Use

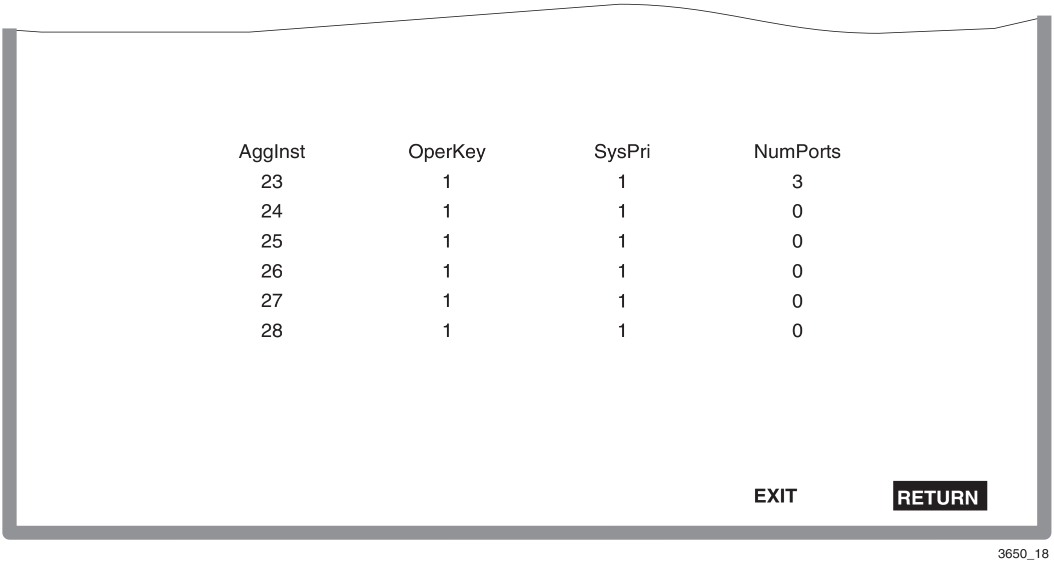
To see a summary of all the available aggregators and other basic information, including the aggregator interface instance, operational key, system priority, and the number of ports currently attached to the aggregator.

How to Access

Use the arrow keys to highlight the **AGGREGATOR** menu item in 802.3ad Main Menu screen and press ENTER. The 802.3ad Aggregator screen, Figure 5-12, displays.

Screen Example

Figure 5-12 802.3ad Aggregator Screen



```
AggInst    OperKey    SysPri    NumPorts
  23          1          1          3
  24          1          1          0
  25          1          1          0
  26          1          1          0
  27          1          1          0
  28          1          1          0
```

Field Descriptions

Refer to Table 5-11 for a functional description of each screen field.

Table 5-11 802.3ad Aggregator Screen Field Descriptions

Use this field…	To…
AggInst (Read-Only)	See dot3adAggIndex, a unique number that identifies this aggregator.
OperKey (Read-Only)	See dot3adAggActorOperKey, the associatedoperational key value.
SysPri (Read-Only)	See dot3adAggActorSystemPriority, the priority value associated with this aggregator.
NumPorts (Read-Only)	See the number of ports that are currently attached to this aggregator.

Viewing and Editing 802.3ad Aggregator Parameters

To view or change Aggregator parameters, proceed as follows:

1. Use the arrow keys to highlight the **parameter field** to be modified and type in the new value. Press ENTER. Repeat this step to change other parameter settings as necessary before saving the new settings.
2. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
3. Press ENTER. The message “SAVED OK” displays. All settings are saved.

Displaying Aggregator Details

To display detail information about an Aggregator, proceed as follows:

1. Use the arrow keys to highlight the **line** containing the Aggregator of interest.
2. Press ENTER. The 802.3ad Aggregator Details screen, described in Section 5.8.2.1, is displayed showing the details of the selected Aggregator.

5.8.2.1 802.3ad Aggregator Details Screen

When to Use

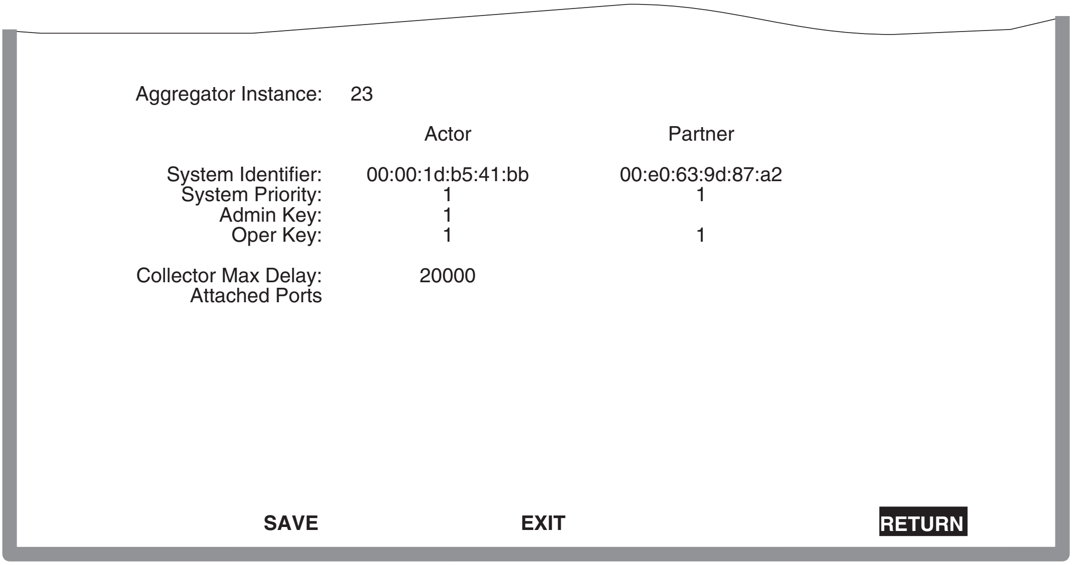
To see the current parameter details of the Aggregator Instance selected on the 802.3ad Aggregator screen described in Section 5.8.2.

How to Access

Use the arrow keys to highlight the **line** containing the Aggregator of interest on the 802.3ad Aggregator screen and press ENTER. The 802.3ad Aggregator Details screen, Figure 5-13, displays.

Screen Example

Figure 5-13 802.3ad Aggregator Details Screen



```
           Aggregator Instance:   23

                                       Actor                  Partner

             System Identifier:   00:00:1d:b5:41:bb      00:e0:63:9d:87:a2
               System Priority:        1                      1
                     Admin Key:        1
                      Oper Key:        1                      1

           Collector Max Delay:      20000
                Attached Ports
```

3650-011_19

Field Descriptions

Refer to Table 5-12 for a functional description of each screen field.

Table 5-12 802.3ad Aggregator Details Screen Field Descriptions

Use this field…	To…
Aggregator Instance	See the instance of the aggregator being viewed. The instance is a numerical value used to uniquely identify an aggregator in a system and matches the aggregator’s logical port number.
Actor	
System Identifier (Read-Only)	See the System associated with the aggregator.
System Priority (Read-Only)	See the system priority value of this aggregator.
Admin Key (Read-Only)	See the Key assigned by management.
Oper Key (Read-Only)	See the current Key being used by the aggregator.
Collector Max Delay (Read-Only)	See the value of this 16-bit read-write attribute, which defines the maximum delay, in tens of microseconds, that may be imposed by the Frame Collector between receiving a frame from an Aggregator Parser, and either delivering the frame to its MAC Client or discarding the frame.
Partner	
System Identifier (Read-Only)	See which system belongs to the remote (partner) aggregator.
System Priority (Read-Only)	See the system priority of the remote aggregator.
Oper Key (Read-Only)	See the operational Key of the remote aggregator.

5.8.3 802.3ad System Screen

When to Use

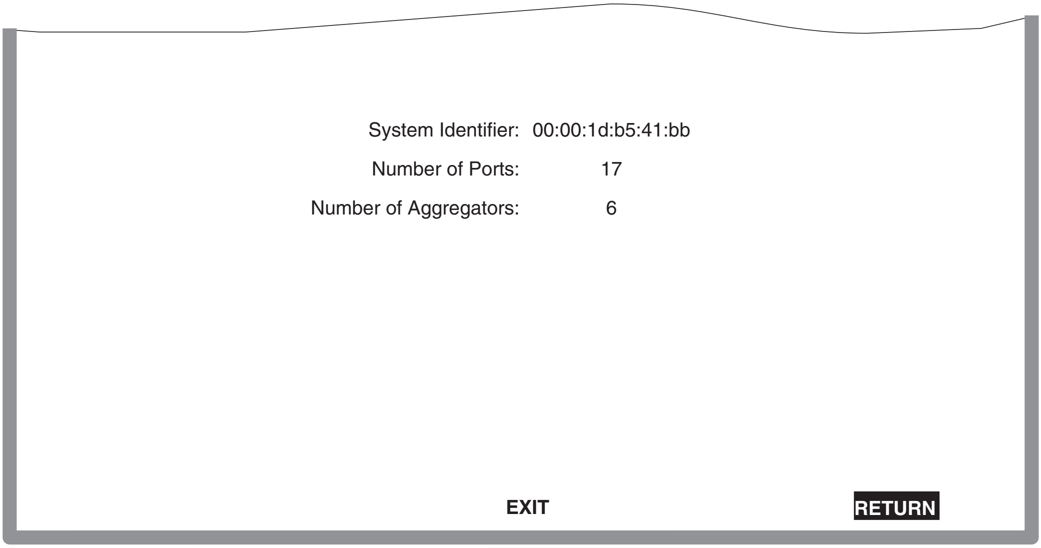
To see basic system-level information, such as System Identifier, Number of Ports and Number of Aggregators.

How to Access

Use the arrow keys to highlight the **SYSTEM** menu item in 802.3ad Main Menu screen and press ENTER. The 802.3ad System screen, Figure 5-14, displays.

Screen Example

Figure 5-14 802.3ad System Screen



```
        System Identifier:  00:00:1d:b5:41:bb
          Number of Ports:        17
    Number of Aggregators:         6
```

3650_20

Field Descriptions

Refer to Table 5-13 for a functional description of each screen field.

Table 5-13 802.3ad System Screen Field Descriptions

Use this field…	To…
System Identifier (Read-Only)	See the uniquely identified system-to-protocol partner.
Number of Ports (Read-Only)	See the number of ports that are participating in 802.3ad on this switch.
Number of Aggregators (Read-Only)	See the number of aggregators that exist on this switch.

5.9 BROADCAST SUPPRESSION CONFIGURATION SCREEN

NOTE: Broadcast frames received above the threshold setting are dropped.

When to Use

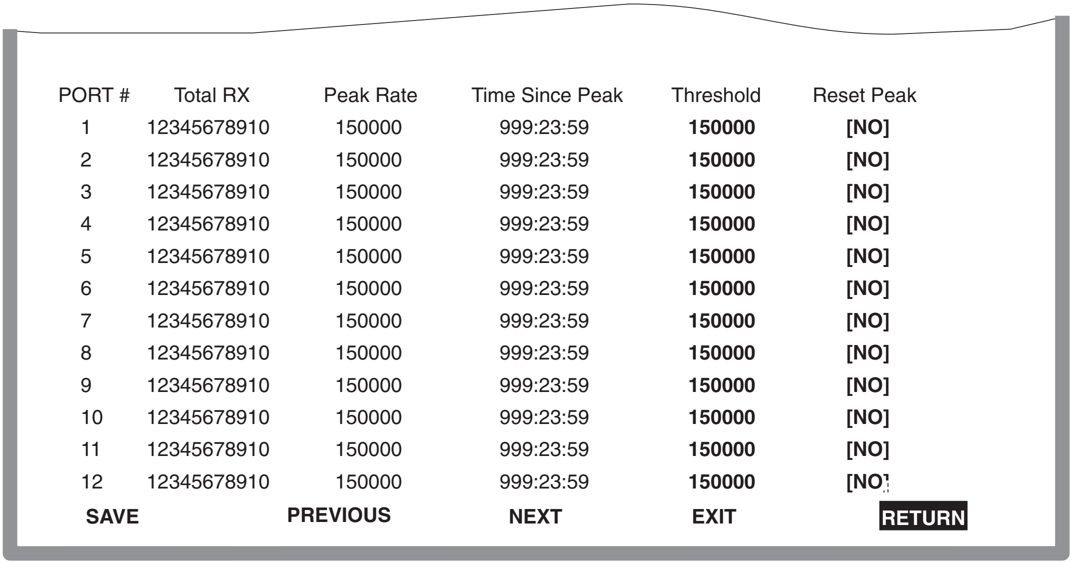
To set the limit on received broadcast frames that are switched out to other ports.

How to Access

Use the arrow keys to highlight the **BROADCAST SUPPRESSION CONFIGURATION** menu item in the Port Configuration Menu screen and press ENTER. The Broadcast Suppression Configuration screen, Figure 5-15, displays.

Screen Example

Figure 5-15 Broadcast Suppression Configuration Screen



PORT #	Total RX	Peak Rate	Time Since Peak	Threshold	Reset Peak
1	12345678910	150000	999:23:59	**150000**	**[NO]**
2	12345678910	150000	999:23:59	**150000**	**[NO]**
3	12345678910	150000	999:23:59	**150000**	**[NO]**
4	12345678910	150000	999:23:59	**150000**	**[NO]**
5	12345678910	150000	999:23:59	**150000**	**[NO]**
6	12345678910	150000	999:23:59	**150000**	**[NO]**
7	12345678910	150000	999:23:59	**150000**	**[NO]**
8	12345678910	150000	999:23:59	**150000**	**[NO]**
9	12345678910	150000	999:23:59	**150000**	**[NO]**
10	12345678910	150000	999:23:59	**150000**	**[NO]**
11	12345678910	150000	999:23:59	**150000**	**[NO]**
12	12345678910	150000	999:23:59	**150000**	**[NO]**

30691_26

Field Descriptions

Refer to Table 5-14 for a functional description of each screen field.

Table 5-14 Broadcast Suppression Configuration Screen Field Descriptions

Use this field…	To…
PORT # (Read-Only)	Identify the number of the port.
Total RX (Read-Only)	See the total number of broadcast frames received.

Table 5-14 Broadcast Suppression Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Peak Rate (Read-Only)	See the highest number of broadcast frames received in a one-second interval.
Time Since Peak (Read-Only)	See the time since peak rate was achieved.
Threshold (Modifiable)	Set the desired limit of receive broadcast frames that will be forwarded per port per second. For details on how to set the threshold, refer to Section 5.9.1.
Reset Peak (Toggle)	Reset the Peak Rate. Resetting the Peak Rate also resets the Time Since Peak field. The Reset Peak field toggles between YES and NO. For details, refer to Section 5.9.2.

5.9.1 Setting the Threshold

To set the Threshold, proceed as follows:

1. Use the arrow keys to highlight the **Threshold** field for the selected port.
2. Type in the numbers for the desired limit. Only enter values in increments of ten (for example; 10, 20, 30, etc.).
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

5.9.2 Setting the Reset Peak

To set the Reset Peak field to YES or NO, proceed as follows:

1. Use the arrow keys to highlight the **Reset Peak** field for the selected port.
2. Press the SPACE bar to select **YES** or **NO**.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays and the Time Since Peak field is also reset.

6

802.1 Configuration Menu Screens

This chapter discusses the Enterasys Networks Rapid Reconvergence Spanning Tree implementation as well as the implementation of IEEE 802.3ad. The following screens are discussed:

- 802.1 Configuration Menu screen (Section 6.1)
- 802.3ad Configuration screens (Chapter 5)
- Spanning Tree Configuration Menu screen (Section 6.2)
  - Spanning Tree Configuration screen (Section 6.3)
  - Spanning Tree Port Configuration screen (Section 6.4)
  - PVST Port Configuration screen (Section 6.5)
- 802.1Q VLAN Configuration Menu screen (Chapter 7)
- 802.1p Configuration Menu screen (Chapter 8)

Screen Navigation Path

Password > Device Menu > Device Configuration Menu > **802.1 Configuration Menu**

6.1 802.1 CONFIGURATION MENU SCREEN

When to Use

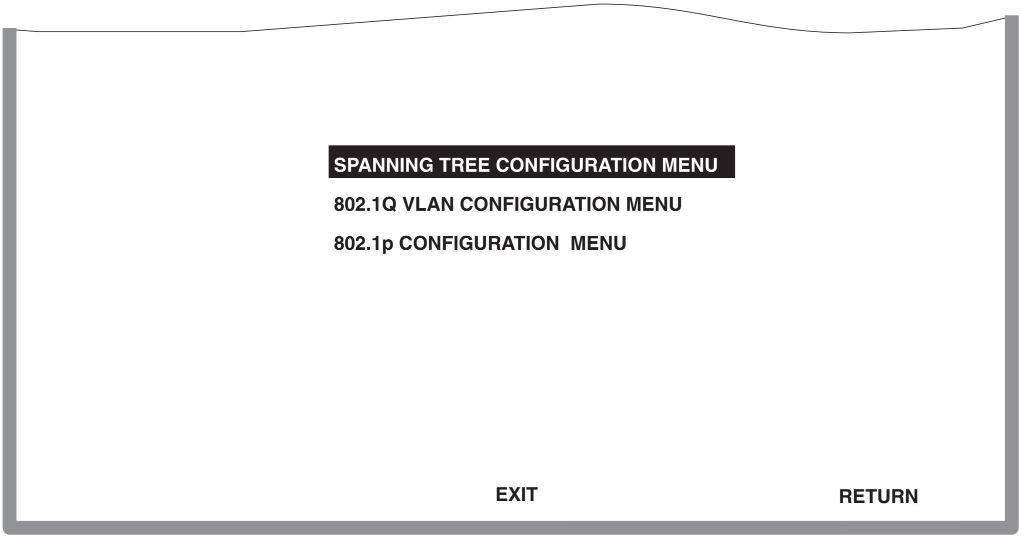
To access the Spanning Tree Configuration Menu, 802.1Q VLAN Configuration Menu, or 802.1p Configuration Menu screen.

How to Access

Use the arrow keys to highlight the **802.1 CONFIGURATION MENU** item on the Device Configuration Menu screen and press ENTER. The 802.1 Configuration Menu screen, Figure 6-1, displays.

Screen Example

Figure 6-1 802.1 Configuration Menu Screen



SPANNING TREE CONFIGURATION MENU

802.1Q VLAN CONFIGURATION MENU

802.1p CONFIGURATION MENU

EXIT RETURN

30691_27

Menu Descriptions

Refer to Table 6-1 for a functional description of each menu item.

Table 6-1 802.1 Configuration Menu Screen Menu Item Descriptions

Menu Item	Screen Function
SPANNING TREE CONFIGURATION MENU	Used to select the Spanning Tree Configuration and Spanning Tree Port Configuration screens. These screens are used for the following functions: • Create a separate Spanning Tree topology for each VLAN configured in the SmartSwitch device. This type of Spanning is referred to as Per VLAN Spanning Tree (PVST). • Configure the switch for Rapid Reconvergence Spanning Tree, which provides faster topology changes, provides less transitioning time to the forwarding state when the SmartSwitch device boots, compatible with PVST, and backwards compatible with traditional IEEE 802.1D. • Enable or disable Spanning Tree on a per port/per VLAN basis. For details, refer to Section 4.2.
802.1Q VLAN CONFIGURATION MENU	Used to select the screens for configuring and managing VLANs. Details about VLANs, how to configure them, and examples showing how to configure the switch for VLANs to solve a given problem are described in Chapter 12. For details about the 802.1Q VLAN Configuration screens, refer to Chapter 7.
802.1p CONFIGURATION MENU	Used to select the Port Priority Configuration, Traffic Class Information, Transmit Queues Configuration, Priority Classification Configuration, and Rate Limiting Configuration screens. For details, refer to Chapter 8.

6.2 SPANNING TREE CONFIGURATION MENU SCREEN

CAUTION: These screens should be used only by personnel who are very knowledgeable about Spanning Trees and how to develop them. Otherwise, the proper operation of the network could be at risk.

Screen Navigation Path

Password > Device Menu > Device Configuration Menu > 802.1 Configuration Menu > **Spanning Tree Configuration Menu**

When to Use

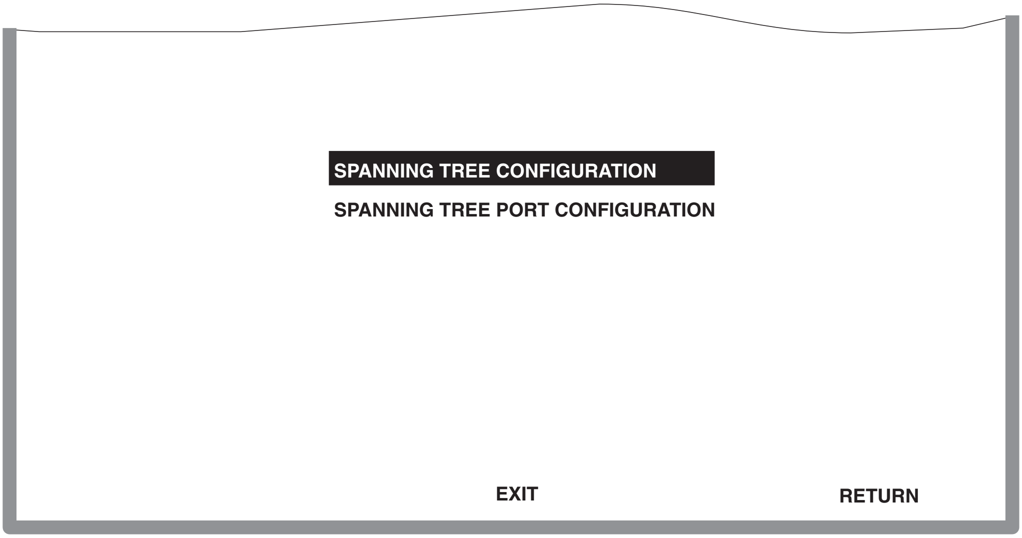
To access the Spanning Tree Configuration, or Spanning Tree Port Configuration screen.

How to Access

Use the arrow keys to highlight the **SPANNING TREE CONFIGURATION MENU** item on the 802.1 Configuration Menu screen and press ENTER. The Spanning Tree Configuration Menu screen, Figure 6-2, displays.

Screen Example

Figure 6-2 Spanning Tree Configuration Menu Screen



30691_28

Menu Descriptions

Refer to Table 6-2 for a functional description of each menu item.

Table 6-2 Spanning Tree Configuration Menu Screen

Menu Item	Screen Function
SPANNING TREE CONFIGURATION	Used to create a Per VLAN Spanning Tree (PVST) instance for each VLAN currently configured on the switch. For details about the Spanning Tree Port Configuration screen, refer to Section 6.3.
SPANNING TREE PORT CONFIGURATION	Used to enable or disable Spanning Tree on a per port, per VLAN basis. For details about the Spanning Tree Port Configuration screen, refer to Section 6.4.
PVST PORT CONFIGURATION	Used to allow Multiple Spanning Trees. This screen displays when you select a port of interest on the **Spanning Tree Port Configuration** screen. For details about the PVST Port Configuration screen, refer to Section 6.5.

6.3 SPANNING TREE CONFIGURATION SCREEN

⚠ **CAUTION:** This screen should be used only by personnel who are very knowledgeable about Spanning Trees and how to develop them. Otherwise, the proper operation of the network could be at risk.

When to Use

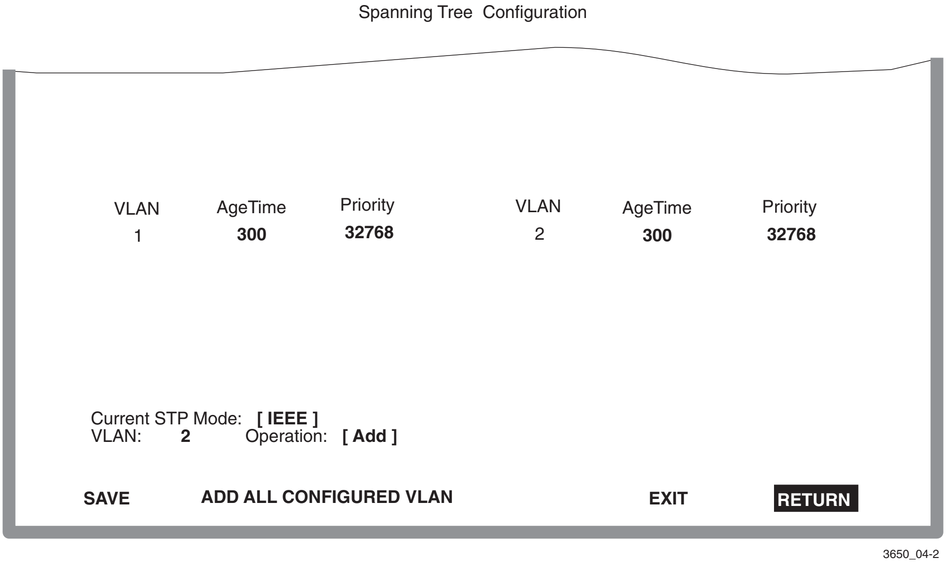
To create a separate Spanning Tree topology for each VLAN configured in the SmartSwitch device and enable/disable the Quick Convergence function on the switch.

How to Access

Use the arrow keys to highlight the SPANNING TREE CONFIGURATION menu item from the Spanning Tree Configuration Menu screen, and press ENTER. The Spanning Tree Configuration screen, Figure 6-3, displays.

Screen Example

Figure 6-3 Spanning Tree Configuration Screen



```
                          Spanning Tree  Configuration

      VLAN      AgeTime      Priority          VLAN      AgeTime      Priority
        1         300         32768              2         300         32768

    Current STP Mode:   [ IEEE ]
    VLAN:      2         Operation:   [ Add ]
```

Field Descriptions

Refer to Table 6-3 for a functional description of each screen field.

Table 6-3 Spanning Tree Configuration Screen

Use this field…	To…
VLAN – top of screen (Read-Only)	See a list of the VLAN or Spanning Tree Instances. This field also enables you to add or delete other VLAN Instances.
AgeTime (Modifiable)	Enter the age time (10 to 1 million seconds) for the associated VLAN. This is the amount of time that the entry remains in the bridge forwarding table. The default is 300.

Table 6-3 Spanning Tree Configuration Screen

Use this field…	To…
Current STP Mode (Selectable)	Select the current STP mode using the SPACE bar. You can select one of the following: IEEE, PVSTP, NONE, and DEC. The default setting is IEEE. It is recommended that all switches in the network be configured for the same STP mode setting. IEEE = 802.1w Spanning Tree protocol – A single spanning tree for the entire network. Redundant links are placed in standby mode. States are predetermined to ensure an accelerated failover. PVSTP = Per VLAN Spanning Tree Protocol – PVSTP is also known as the Spanning Forest. PVSTP allows each VLAN to have its own spanning tree, which allows multiple links to be active, each assigned to a different VLAN. NONE = Spanning tree is not enabled. DEC = DEC spanning tree protocol.
Priority (Selectable)	Select the VLAN’s 802.1D bridge priority using the SPACE bar. Valid values are in multiples of 4096, with 0 indicating high priority. Default value is 32768. The VLAN with the highest priority becomes the Spanning Tree root.
VLAN – bottom of screen (Modifiable)	Enter the number of the VLAN to be added or deleted from the VLAN list. The default value is 2.
Operation (Toggle)	Add or Delete the VLAN entered in the VLAN field. This field is toggled using the SPACE bar. The default value is Add.
ADD ALL CONFIGURED VLAN (Toggle)	Implement the new configuration to all static VLANs and update the VLAN list to include the new static VLANs.

6.3.1 Configuring a VLAN Spanning Tree

To configure a VLAN Spanning Tree, proceed as follows:

1. Use the arrow keys to highlight the **Current STP Mode** field near the bottom of the screen.
2. Use the SPACE bar to select one of the following: IEEE, PVSTP, NONE, and DEC. The default setting is IEEE.
3. Use the arrow keys to highlight the **VLAN** field near the bottom of the screen.
4. Type in the number of the VLAN that you want to add or delete from the Spanning Tree. This establishes the STP VLAN ID of the VLAN.
5. Use the arrow keys to highlight the **Operation** field near the bottom of the screen.
6. Use the SPACE bar to select Add or Delete.
7. Press ENTER. The VLAN entered in the VLAN field is added or deleted from the list accordingly. When a VLAN is added, the age time default value of 300 seconds, and the bridge priority value of 32768, are automatically set.
8. If you want to change the age time of the VLAN, use the arrow keys to highlight the **Age Time** field.
9. Type in the appropriate age time. A time from 10 to 1 million seconds may be entered.
10. If you want to change the priority value of the VLAN, use the arrow keys to highlight the **Priority** field.
11. Use the SPACE bar to select a priority value.
12. If more than one VLAN is to be added/deleted, repeat steps 4 through 11 until all VLANs are configured before saving the settings.
13. Use the arrow keys to highlight the **SAVE** command and press ENTER to save all your settings at once.
14. If you want to add all the VLANs configured on the switch to the screen with a default age time of 300 seconds and a bridge priority of 32768, use the arrow keys to highlight the **ADD ALL CONFIGURED VLAN** command and press ENTER.

6.4 SPANNING TREE PORT CONFIGURATION SCREEN

CAUTION: This screen should be used only by personnel who are very knowledgeable about Spanning Trees and how to develop them. Otherwise, the proper operation of the network could be at risk.

When to Use

To view the switch address of the selected STP VLAN ID, its VLAN age time, the total number of ports, and the current MAC Address of a switch residing of each port.

The Spanning Tree Port Configuration screen is also used to allow or prevent ports from participating in the default STP VLAN.

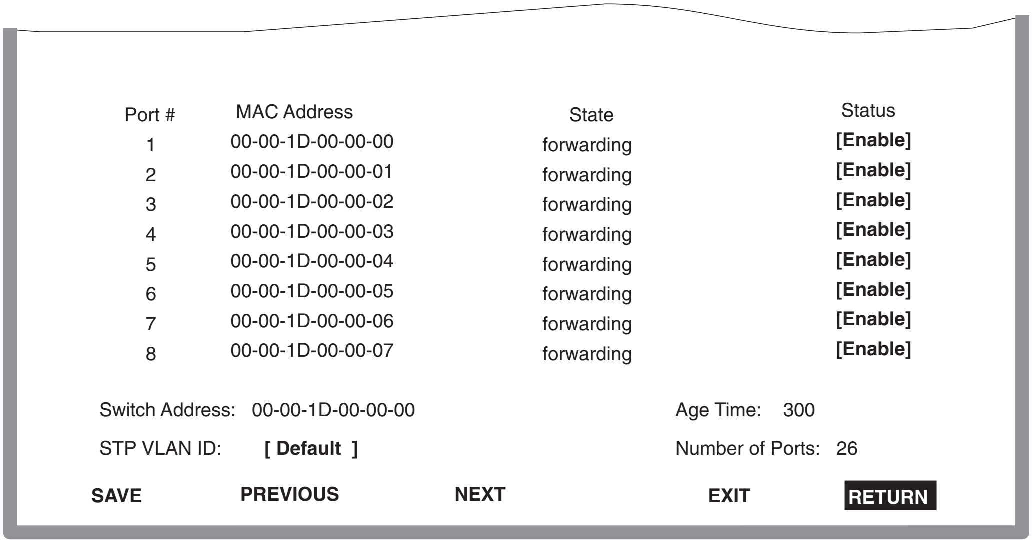
This screen also provides access to the PVST Configuration screen.

How to Access

Use the arrow keys to highlight the SPANNING TREE PORT CONFIGURATION menu item on the Spanning Tree Configuration Menu screen, and press ENTER. The Spanning Tree Port Configuration screen, Figure 6-4, displays.

Screen Example

Figure 6-4 Spanning Tree Port Configuration Screen



Port #	MAC Address	State	Status
1	00-00-1D-00-00-00	forwarding	**[Enable]**
2	00-00-1D-00-00-01	forwarding	**[Enable]**
3	00-00-1D-00-00-02	forwarding	**[Enable]**
4	00-00-1D-00-00-03	forwarding	**[Enable]**
5	00-00-1D-00-00-04	forwarding	**[Enable]**
6	00-00-1D-00-00-05	forwarding	**[Enable]**
7	00-00-1D-00-00-06	forwarding	**[Enable]**
8	00-00-1D-00-00-07	forwarding	**[Enable]**

Switch Address: 00-00-1D-00-00-00 Age Time: 300

STP VLAN ID: **[Default]** Number of Ports: 26

Field Descriptions

Refer to Table 6-4 for a functional description of each screen field.

Table 6-4 Spanning Tree Port Configuration Screen

Use this field…	To…
Port # (Read-Only)	See the port numbers of each link associated with the STP VLAN ID selected in the STP VLAN ID field.
MAC Address (Read-Only)	See the Mac address of the switch residing of each port.The first MAC Address is always associated with the VLAN ID selected in the STP VLAN ID field. The default is the MAC Address of the Default VLAN.
State (Read-Only)	See the current state of each port; listening, learning, or forwarding.
Status (Toggle/Read-Only)	Enable or disable the physical state of the ports. The Status field toggles between Enable and Disable using the SPACE bar. When you step to an STP VLAN ID other than Default, this field becomes a read-only field that shows the status of the ports associated with the VLAN shown in the STP VLAN ID field.
Switch Address (Read-Only)	See the MAC address of the switch.
Age Time (Read-Only)	See the age time of learned entries.
STP VLAN ID (Selectable)	Select the STP VLAN ID. You can step this field to the STP VLAN IDs of each existing VLAN by using the SPACE bar. The default setting is Default, which represents the Default VLAN, 1. When you highlight the STP VLAN ID field and press ENTER, the number of ports of the STP VLAN ID and their current status are displayed.
Number of Ports (Read-Only)	See the total number ports associated with the VLAN ID selected in the STP VLAN ID field. This field changes when you highlight the STP VLAN ID field and press ENTER.

6.4.1 Enabling/Disabling the Default Spanning Tree Ports

CAUTION: The Spanning Tree configuration should be done only by personnel who are very knowledgeable about Spanning Trees and how to develop them. Otherwise, the proper operation of the network could be at risk.

Ports associated with the Default STP VLAN can be enabled or disabled, as follows:

1. To enable or disable a port, use the arrow keys to highlight the **Status** field associated with that port.
2. Use the SPACE bar to toggle to either Enable or Disable the port.
3. Use the arrow keys to highlight the **SAVE** command and press ENTER to save all your settings at once.

6.4.2 Viewing Status of Spanning Tree Ports

Ports and their status associated with an STP VLAN can be viewed, as follows:

1. Use the arrow keys to highlight the **STP VLAN ID** field near the bottom of the screen.
2. Use the SPACE bar to step to the appropriate STP VLAN ID and press ENTER. The ports, MAC Address, port state, port status, age time, and number of ports associated with the STP VLAN ID are displayed.
3. If there are more than eight ports associated with a VLAN, you can use the NEXT command at the button of the screen to see the next eight ports.

6.5 PVST PORT CONFIGURATION SCREEN

When to Use

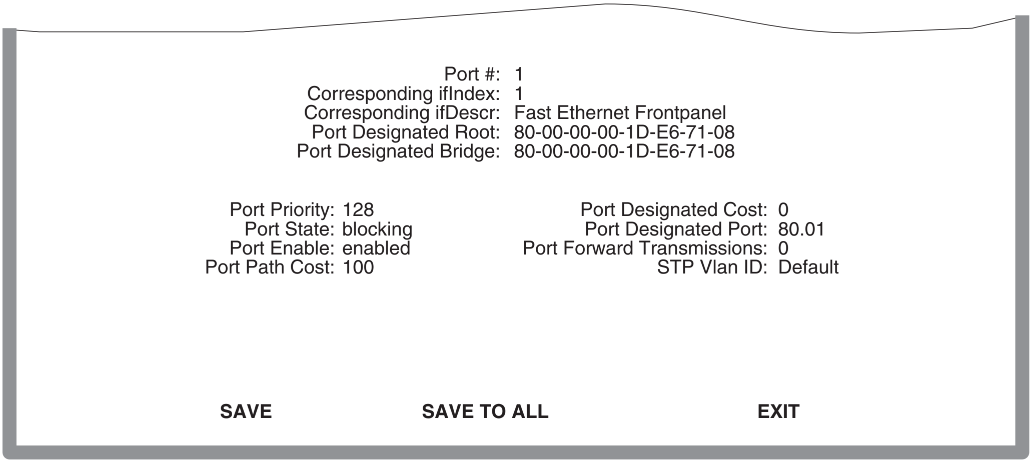
To change the configuration parameters of a selected PVST port.

How to Access

Use the arrow keys to highlight the port of interest on the **Spanning Tree Port Configuration** screen, then press ENTER. The PVST Port Configuration screen, Figure 6-5, displays.

Screen Example

Figure 6-5 PVST Port Configuration Screen



```
                      Port #:  1
       Corresponding ifIndex:  1
       Corresponding ifDescr:  Fast Ethernet Frontpanel
        Port Designated Root:  80-00-00-00-1D-E6-71-08
      Port Designated Bridge:  80-00-00-00-1D-E6-71-08

  Port Priority:  128                   Port Designated Cost:  0
     Port State:  blocking              Port Designated Port:  80.01
    Port Enable:  enabled         Port Forward Transmissions:  0
 Port Path Cost:  100                           STP Vlan ID:  Default
```

Field Descriptions

Refer to Table 6-5 for a functional description of each screen.

Table 6-5 PVST Port Configuration Screen Field Descriptions

Use this field…	To…
Port # (Read-Only)	View the bridge port number of this port.
Corresponding ifindex (Read-Only)	View the corresponding interface number for this port.
Corresponding idDescr (Read-Only)	View the interface description for this port.
Port Designated Root (Read-Only)	View the bridge ID of the bridge considered root by the designated bridge of the segment to which this port is attached.
Port Designated Bridge (Read-Only)	View the bridge ID of the bridge this port considers to be designated bridge for this port's segment.

Table 6-5 PVST Port Configuration Screen Field Descriptions

Use this field…	To…
Port Priority (Modifiable)	View the value of the priority portion of the port ID.
Port Designated Cost (Read-Only)	View the path cost of the designated port of this port's segment.
Port State (Read-Only)	View the current Spanning Tree state of this port.
Port Designated Port (Read-Only)	View the port id of the port on the designated bridge for this port's segment.
Port Enable (Read-Only)	View the status of the port (enabled/disabled).
Port Forward Transmissions (Read-Only)	View the number of times this port has transitioned from the learning state to the forwarding state.
Port Path Cost (Modifiable)	View the cost contribution of this port in the path to the Spanning Tree root.
STP Vlan ID (Read-Only)	View the ID of the VLAN in which this port belongs.

7

802.1Q VLAN Configuration Menu Screens

NOTE: It is strongly recommended that you read Chapter 12 to gain an understanding of VLANs and the associated terminology; how to use the VLAN Configuration screens to create VLANs; examples of how to configure VLANs in switches to solve a problem; and details on how frames are handled as they travel through the network.

This chapter describes the 802.1Q VLAN Configuration Menu screen (Section 7.2) and the following screens that can be selected from its menu:

- Static VLAN Configuration screen (Section 7.3)
  - Static VLAN Egress Configuration screen (Section 7.4)
- Current VLAN Configuration screen (Section 7.5)
  - Current VLAN Egress Configuration screen (Section 7.6)
- VLAN Port Configuration screen (Section 7.7)
- VLAN Classification Configuration screen (Section 7.8)
  - Protocol Port Configuration (Section 7.9)

Screen Navigation Path

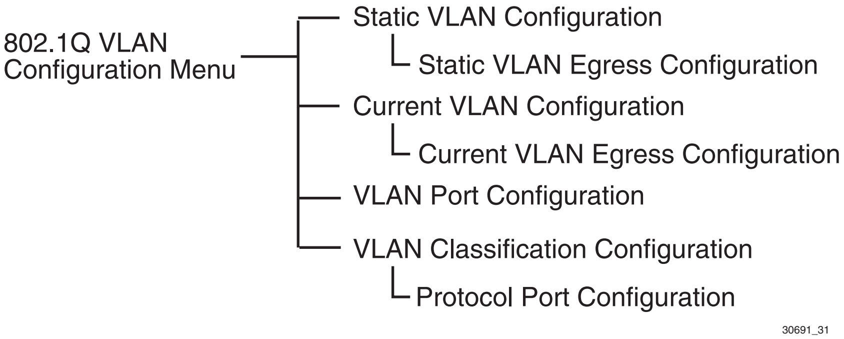
Password > Device Menu > Device Configuration Menu > 802.1 Configuration Menu > **802.1Q VLAN Configuration Menu**

7.1 SUMMARY OF VLAN LOCAL MANAGEMENT

The VLAN configuration process is an extension of normal Local Management operations. A series of Local Management screens provides access to the functions and commands necessary to add, change, or delete VLANs and to assign ports to those VLANs.

The VLAN configuration screens are a standard part of the Local Management hierarchy when the switch is configured to operate in 802.1Q Mode. The hierarchy of the Local Management screens pertaining to 802.1Q VLAN configuration is shown in Figure 7-1.

Figure 7-1 802.1Q VLAN Screen Hierarchy


802.1Q VLAN Configuration Menu
Static VLAN Configuration
Static VLAN Egress Configuration
Current VLAN Configuration
Current VLAN Egress Configuration
VLAN Port Configuration
VLAN Classification Configuration
Protocol Port Configuration
30691_31

7.1.1 Preparing for VLAN Configuration

Some forethought and planning is essential to a good VLAN implementation. Before attempting to configure a single switch for VLAN operation, consider the following:

- How many VLANs will be required?
- What stations will belong to them?
- What ports are connected to those stations?
- What ports will be configured as GARP-aware ports?

It is also helpful to sketch out a diagram of your VLAN strategy. The examples provided in Chapter 12 are useful depictions of the planning process.

To configure the switch for VLAN operation, proceed as follows:

- Access Local Management as described in Chapter 3.
- Perform all required initial setup operations.
- Navigate to the 802.1Q VLAN Configuration Menu screen to begin the VLAN configuration process for the switch.

7.2 802.1Q VLAN CONFIGURATION MENU SCREEN

When to Use

To select screens to assign switched network ports to static VLANs, define new VLANs, and configure port filtering according to a VLAN list. Network users can be logically grouped into VLANs even if they span long physical distances over a vast, intricate physical network.

The VLAN Local Management menu items listed on the 802.1Q VLAN Configuration Menu screen allow such VLANs to be configured on a network at the switched port of the SmartSwitch device. Each port mode of operation can also be configured to handle untagged frames (Hybrid Mode), tagged frames (1Q Trunk Mode), or frames of a legacy 802.1D switch fabric (1D Trunk Mode). Also, some or all of the ports on the switch can be configured as GVRP ports, which enables dynamic VLAN registration. This keeps the traffic associated with a particular VLAN and protocol to be isolated from the other parts of the network.

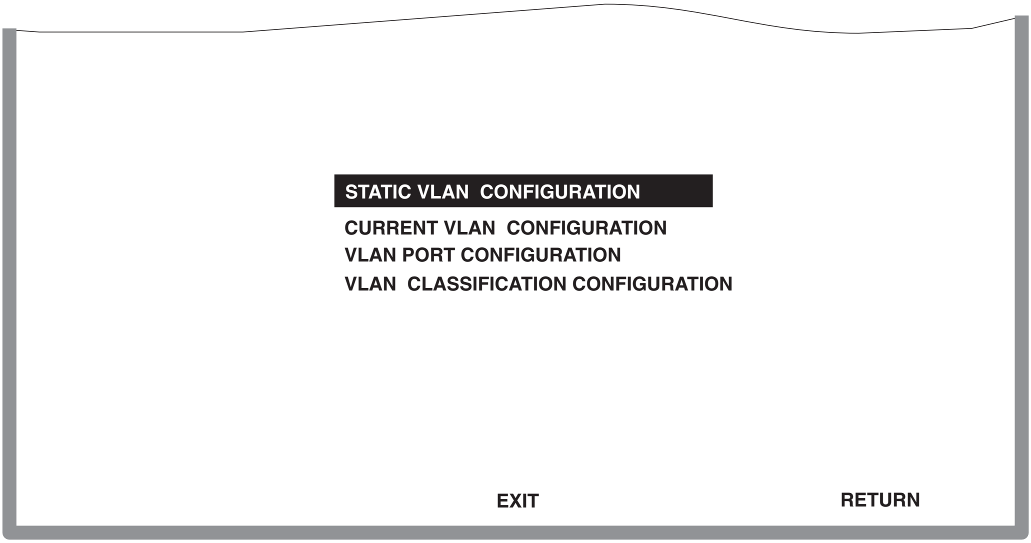
NOTE: There is a global setting for GVRP that is enabled by default. Refer to Table 7-6 for more information.

How to Access

Use the arrow keys to highlight the **802.1Q VLAN CONFIGURATION MENU** item on the 802.1 Configuration Menu screen and press ENTER. The 802.1Q VLAN Configuration Menu screen, Figure 7-2, displays.

Screen Example

Figure 7-2 802.1Q VLAN Configuration Menu Screen


STATIC VLAN CONFIGURATION
CURRENT VLAN CONFIGURATION
VLAN PORT CONFIGURATION
VLAN CLASSIFICATION CONFIGURATION
EXIT
RETURN

30691_32

Menu Descriptions

Refer to Table 7-1 for a functional description of each menu item.

Table 7-1 802.1Q VLAN Configuration Menu Screen Menu Item Descriptions

Menu Item	Screen Function
STATIC VLAN CONFIGURATION	Used to view, add, name, enable, or disable static VLANs within the SmartSwitch device, and also display the Filter Database ID (FDB ID) associated with each VLAN. This screen also allows you to access the Static VLAN Egress Configuration screen. The Static VLAN Egress Configuration screen enables you to set one or more ports associated with a VLAN to transmit frames according to an egress setting (UNTAGGED, TAGGED, or NO). For more information on the Static VLAN Configuration screen, refer to Section 7.3. For more information on the Static VLAN Egress Configuration screen, refer to Section 7.4.
CURRENT VLAN CONFIGURATION	Displays a list of the current VLANs along with their VLAN IDs, FDB IDs, VLAN Type, and if they have ports on the egress list. Each VLAN ID on the list may be highlighted to access the Current VLAN Egress Configuration screen. This screen provides a list and Egress status of each port associated with the selected VLAN. For more information on the Current VLAN Configuration screen, refer to Section 7.5. For more information on the Current VLAN Egress Configuration screen, refer to Section 7.6.
VLAN PORT CONFIGURATION	Used to view a list of ports and enables you to configure each port to either receive all frames or only tagged frames, set the PVID, enable or disable ingress filtering on each port, and enable or disable GVRP on each port. For more information on the VLAN Port Configuration screen, refer to Section 7.7. For more information on GVRP, refer to Appendix A.

Table 7-1 802.1Q VLAN Configuration Menu Screen Menu Item Descriptions (Continued)

Menu Item	Screen Function
VLAN CLASSIFICATION CONFIGURATION	Used to display the current entries of VLAN ID (VID), protocol classification, and description of each classification; assign VLANs according to Classification rules; add/delete a VID and associated classification entry; and access the Protocol Port Configuration screen. Refer to Section 7.8 for additional information.

7.3 STATIC VLAN CONFIGURATION SCREEN

When to Use

To create, modify, and/or delete one or more Static VLANs and associated VLAN names. This screen also provides access to the Static VLAN Egress Configuration screen to modify the port list of a VLAN selected from this screen, as described in Section 7.3.2.

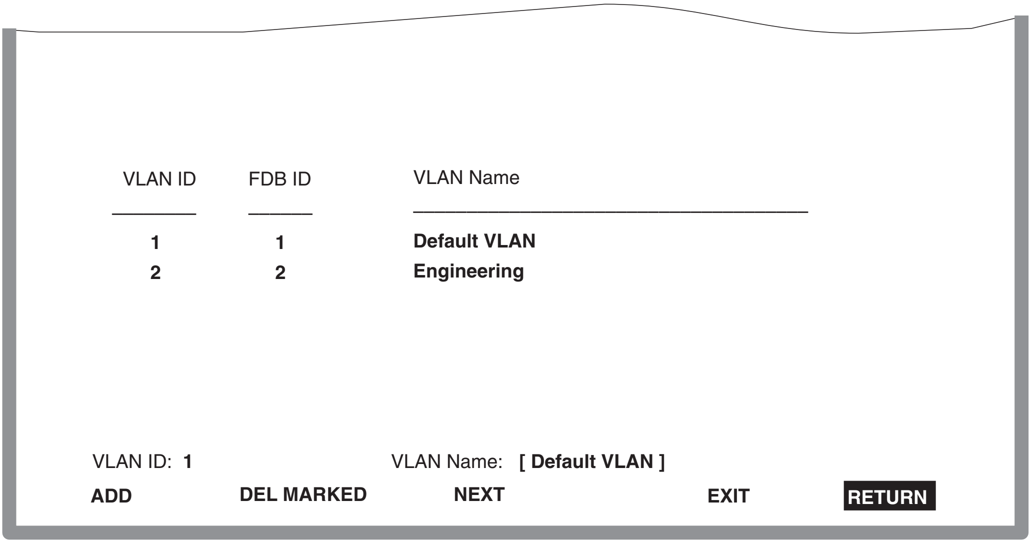
NOTE: Static VLANs are those VLANs that you create manually using this screen and can only be deleted using this screen.

How to Access

Use the arrow keys to highlight the **STATIC VLAN CONFIGURATION** menu item on the 802.1Q VLAN Configuration Menu screen, and press ENTER. The Static VLAN Configuration screen (Figure 7-3) displays.

Screen Example

Figure 7-3 Static VLAN Configuration Screen



```
     VLAN ID       FDB ID          VLAN Name
    ________       ______          ______________________________________
        1            1             Default VLAN
        2            2             Engineering




   VLAN ID:  1                   VLAN Name:   [ Default VLAN ]
   ADD            DEL MARKED        NEXT                 EXIT          RETURN
```

30691_33

Field Descriptions

Refer to Table 7-2 for a functional description of each screen field. Refer to Section 7.3.1 through Section 7.3.5 for the application of these fields.

Table 7-2 Static VLAN Configuration Screen Field Descriptions

Use this field…	To…
VLAN ID – top of screen (Read-Only)	See the assigned VLAN IDs that are configured in the SmartSwitch device. Initially, only the Default VLAN (VLAN ID: 1) is listed. Up to ten VLANs can be displayed in the screen. If there are more than ten VLANs, the NEXT command appears at the bottom of the screen to allow stepping to the next screen.
FDB ID (Read-Only)	See the Filter Database ID (FDB ID) numbers of the associated VLAN IDs. This value is allocated automatically by the device when the VLAN is created: either dynamically by GVRP, or when a Static VLAN is created using this screen.

Table 7-2 Static VLAN Configuration Screen Field Descriptions (Continued)

Use this field…	To…
VLAN Name – top of screen (Read-Only)	See the VLAN Name of the associated VLAN ID. If a name has not been assigned to a VLAN, no name is displayed in the VLAN Name field.
VLAN ID – bottom of screen (Modifiable)	Enter a VLAN ID (VID) number (2 to 4094) for the new VLAN. Up to 1024 VLANs are supported by the SmartSwitch device.
VLAN Name – bottom of screen (Modifiable)	Assign or change names of VLANs. The VLAN Name (with up to 32 characters) is an optional attribute of a VLAN, and is not required for VLAN operation.
ADD (Command)	Add the new VLAN to the SmartSwitch device. If this is successful, the screen refreshes and the new VLAN is added to the list in the screen.
DEL MARKED (Command)	Delete the VLANs shown in the screen marked with an asterisk to the left of the VLAN ID number. The Default VLAN cannot be marked and deleted.

7.3.1 Creating a Static VLAN

To create a VLAN, proceed as follows:

1. Use the arrow keys to highlight the **VLAN ID** field near the bottom of the screen.
2. Enter the VLAN ID using a unique number between 2 and 4094. The VLAN IDs of 0, 1, and 4095 may not be used for user-defined VLANs.

NOTE: Each VLAN ID must be unique. If a duplicate VLAN ID is entered, the switch assumes that the Administrator intends to modify the existing VLAN.

3. Press ENTER. If an illegal number is entered, the Event Message Line will display: “PERMISSIBLE RANGE FOR VLAN IDS: 2 to 4094” and the field will refresh with the previous value.

4. Use the arrow keys to highlight the **VLAN Name** field.
5. Type a name of up to 32 ASCII characters in the VLAN Name field. This is an optional attribute and is not required for VLAN operation.
6. Press ENTER.
7. Use the arrow keys to highlight the **ADD** field near the bottom of the screen.
8. Press ENTER. If the VLAN is successfully created, the screen refreshes and shows the newly created VLAN. If the VLAN is not created successfully, an error is displayed in the Event Message Line at the top of the screen.

7.3.2 Displaying the Current Static VLAN Port Egress List

To see the ports associated with a particular VLAN, the Static VLAN Egress Configuration screen must be displayed. This screen is also used to change the Egress setting for each port of the VLAN. For more information about the Static VLAN Egress Configuration screen, refer to Section 7.4.

To access the Static VLAN Egress Configuration screen, proceed as follows:

1. Use the arrow keys to step to the **line** with the VLAN of interest.
2. Press ENTER. The Static VLAN Egress Configuration screen displays, showing a list of the current ports associated with the VLAN selected in step 1. For more information about the Static VLAN Egress Configuration screen and how to use it, refer to Figure 7-4.

7.3.3 Renaming a Static VLAN

To change the name of an existing VLAN, proceed as follows:

1. Use the arrow keys to highlight the **VLAN ID** field near the bottom of the screen.
2. Type the VLAN ID number of the VLAN to be changed. Press ENTER.
3. Use the arrow keys to highlight the **VLAN Name** field near the bottom of the screen.
4. Type the new VLAN name of up to 32 ASCII characters in the VLAN Name field.
5. Press ENTER.
6. Use the arrow keys to highlight the ADD field and press ENTER. The new name is now displayed.

7.3.4 Deleting a Static VLAN

To delete a VLAN from the VLAN list, proceed as follows:

1. Use the arrow keys to highlight the line containing the VLAN ID, FDB ID, and VLAN Name information. The following message is displayed at the top of the screen:
   "Hit <RETURN> key to edit port list, or <M> to mark."

NOTE: The default VLAN cannot be deleted from the list.

2. Press the **M** (not case sensitive) key, and an asterisk (*) appears to the left of the highlighted line.

   If more than one VLAN is to be deleted, repeat steps 1 and 2 to highlight and mark each line. Otherwise, go to step 4.

NOTE: If for some reason you want to remove a mark, perform steps 1 and 2 to mark the line. Then press **M** to delete the mark.

3. After the lines are marked, use the arrow keys to highlight the DEL MARKED command.
4. Press ENTER. The VLANs and marked line items are deleted from the list.

7.3.5 Paging Through the VLAN List

To display additional VLANs that do not display in the current VLAN List as shown on the screen, use the **NEXT** or **PREVIOUS** commands located at the bottom of the screen, as follows:

NOTE: The NEXT and PREVIOUS fields will only display if there are further VLAN List entries to page through.

1. To display the next screen, use the arrow keys to highlight **NEXT**. Press ENTER to view the entries on the next screen.
2. To display the previous screen, use the arrow keys to highlight **PREVIOUS**. Press ENTER to view the entries on the previous screen.

7.4 STATIC VLAN EGRESS CONFIGURATION SCREEN

When to Use

To set the type of egress (tag status) for each or all ports associated with a VLAN selected from the Static VLAN Configuration screen. The ports can be set using the following selections:

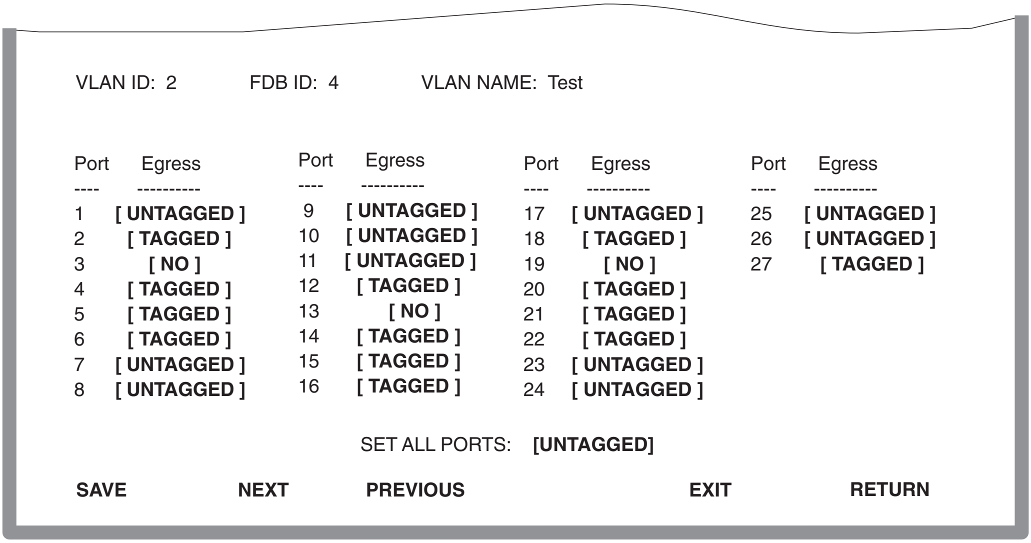
- **UNTAGGED** – sets the port to transmit frames without a tag header. This setting is usually set to configure a port connected to an end user device.
- **TAGGED** – sets the port to transmit frames with a tag header to associate the frame with the VLAN. This setting is usually to configure a port as a trunk port to another switch.
- **NO** – sets the port so it does not transmit frames (tagged or untagged) of the VLAN.

How to Access

Use the arrow keys to highlight the line item with the VLAN ID of interest on the Static VLAN Configuration screen and press ENTER. The Static VLAN Egress Configuration screen, Figure 7-4, displays.

Screen Example

Figure 7-4 Static VLAN Egress Configuration Screen



```
VLAN ID:  2          FDB ID:  4          VLAN NAME:  Test


Port    Egress           Port    Egress           Port    Egress           Port    Egress
----    ----------       ----    ----------       ----    ----------       ----    ----------
1    [ UNTAGGED ]        9    [ UNTAGGED ]        17   [ UNTAGGED ]        25   [ UNTAGGED ]
2      [ TAGGED ]        10   [ UNTAGGED ]        18     [ TAGGED ]        26   [ UNTAGGED ]
3        [ NO ]          11   [ UNTAGGED ]        19       [ NO ]          27     [ TAGGED ]
4      [ TAGGED ]        12     [ TAGGED ]        20     [ TAGGED ]
5      [ TAGGED ]        13       [ NO ]          21     [ TAGGED ]
6      [ TAGGED ]        14     [ TAGGED ]        22     [ TAGGED ]
7    [ UNTAGGED ]        15     [ TAGGED ]        23   [ UNTAGGED ]
8    [ UNTAGGED ]        16     [ TAGGED ]        24   [ UNTAGGED ]

                          SET ALL PORTS:   [UNTAGGED]

SAVE           NEXT          PREVIOUS                     EXIT            RETURN
```

30691_34

Field Descriptions

Refer to Table 7-3 for a functional description of each screen field.

Table 7-3 Static VLAN Egress Configuration Screen Field Descriptions

Use this field…	To…
VLAN ID (Read-Only)	See the VLAN ID of the VLAN selected in the Static VLAN Configuration screen.
FDB ID (Read-Only)	See the Filter Database ID (FDB ID) number associated with the VLAN ID.
VLAN Name (Read-Only)	See the VLAN Name associated with the VLAN ID.
Port (Read-Only)	See a list of ports associated with the VLAN ID. Up to 32 ports may be listed on the screen. If more than 32 ports are associated with a VLAN ID, the NEXT command is displayed to step to the next screen.
Egress (Selectable)	Select the type of VLAN frame transmission (egress) for each port. You can select UNTAGGED, TAGGED or NO using the SPACE bar. **UNTAGGED** – the port will only transmit the VLAN frames as untagged. **TAGGED** – the port will only transmit the VLAN frames as tagged. **NO** – the port is removed from the VLAN Egress List, so that the port will not transmit the VLAN frames. If NO appears without brackets and not in bold type, the port setting cannot be changed directly using this screen, but has virtual ports such as that of a physical ATM port (i.e., an ATM physical port can have more than one virtual port, which can be configured using its own local management). Initially, the default setting is UNTAGGED. When a new VLAN is created, the default setting is NO on all ports.
SET ALL PORTS (Selectable)	Set all ports to the same setting. You can select UNTAGGED, TAGGED, or NO, using the SPACE bar. The default setting is UNTAGGED.

7.4.1 Setting Egress Types on Ports

The following procedures describe how to assign the egress type to one or more ports, or set one egress type to all ports simultaneously.

Setting the Egress Type on One or More Ports Individually

1. Use the arrow keys to highlight the Egress field adjacent to the Port number. The port type is displayed (i.e., Fast Ethernet Frontpanel, Gigabit Ethernet VHSIM, etc.) at the top of the screen.

2. Press the SPACE bar to step to the appropriate Egress field (**UNTAGGED**, **TAGGED**, or **NO**) for the port.

UNTAGGED – sets the port to transmit the VLAN frames without a tag header.

TAGGED – sets the port to transmit frames with a tag header to associate the frame with the VLAN.

NO – the port supports tagging, but is shut down so that no frames of the VLAN are transmitted.

3. To change the egress type on more than one port, repeat the first two steps for each port.

4. After the changes are complete, use the arrow keys to highlight the **SAVE** command at the bottom of the screen.

5. Press ENTER. The message “SAVED OK” displays and the settings are saved.

Setting the Same Egress Type on All Ports Simultaneously

1. Use the arrow keys to highlight the **SET ALL PORTS** field. The following message displays at the top of the screen:

TOGGLE TO DESIRED SELECTION AND HIT <RETURN> TO PROPAGATE SELECTION TO PORTS

2. Press the SPACE bar to step to the appropriate egress type (**UNTAGGED**, **TAGGED**, or **NO**). and press ENTER.

3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.

4. Press ENTER. The message “SAVED OK” displays and the screen refreshes showing all ports associated with the VLAN that are set to the selected egress type.

7.4.2 Displaying the Next Group of Ports

Up to 32 ports can be displayed on the screen. If there are more than 32 ports associated with the VLAN, additional screens will contain the additional list of ports.

NOTE: The NEXT and PREVIOUS fields will only display if there are further egress lists to page through.

To display the additional port settings that do not display in the current screen, use the **NEXT** or **PREVIOUS** commands, as follows:

1. To display the next screen, use the arrow keys to highlight **NEXT**. Press ENTER to view the entries on the next screen.
2. To display the previous screen, use the arrow keys to highlight **PREVIOUS**. Press ENTER to view the entries on the previous screen.

7.5 CURRENT VLAN CONFIGURATION SCREEN

When to Use

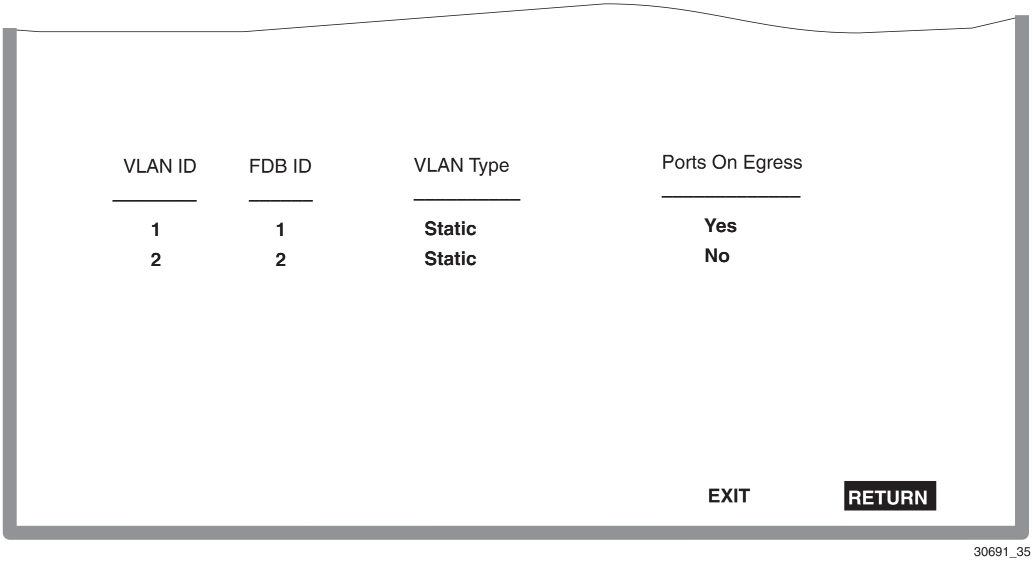
To see the current VLANs and the associated FDB ID, VLAN type, and if the ports are on the egress list. The egress list is the way the switch keeps track of all VLANs that it will recognize.

How to Access

Use the arrow keys to highlight the **CURRENT VLAN CONFIGURATION** menu item on the 802.1Q VLAN Configuration Menu screen, and press ENTER. The Current VLAN Configuration screen, Figure 7-5, displays.

Screen Example

Figure 7-5 Current VLAN Configuration Screen



VLAN ID	FDB ID	VLAN Type	Ports On Egress
1	1	Static	Yes
2	2	Static	No

Field Descriptions

Refer to Table 7-4 for a functional description of each screen field.

NOTE: These fields are read-only fields, however, highlighting a line using the arrow keys and pressing ENTER causes the Current VLAN Egress Configuration screen to display. That screen shows the egress setting for each port associated with the VLAN ID in the highlighted line.

Table 7-4 Current VLAN Configuration Screen Field Descriptions

Use this field…	To…
VLAN ID (Read-Only)	See a list of the VLANs currently recognized by the switch.
FDB ID (Read-Only)	See the Filter Database ID (FDB ID) of the associated VLAN.
VLAN Type (Read-Only)	See the VLAN Type of the associated VLAN (Static or Dynamic). An example of a dynamic VLAN is a GVRP VLAN.

Table 7-4 Current VLAN Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Ports On Egress (Read-Only)	See if the ports associated with each VLAN are on the egress list.

7.6 CURRENT VLAN EGRESS CONFIGURATION SCREEN

When to Use

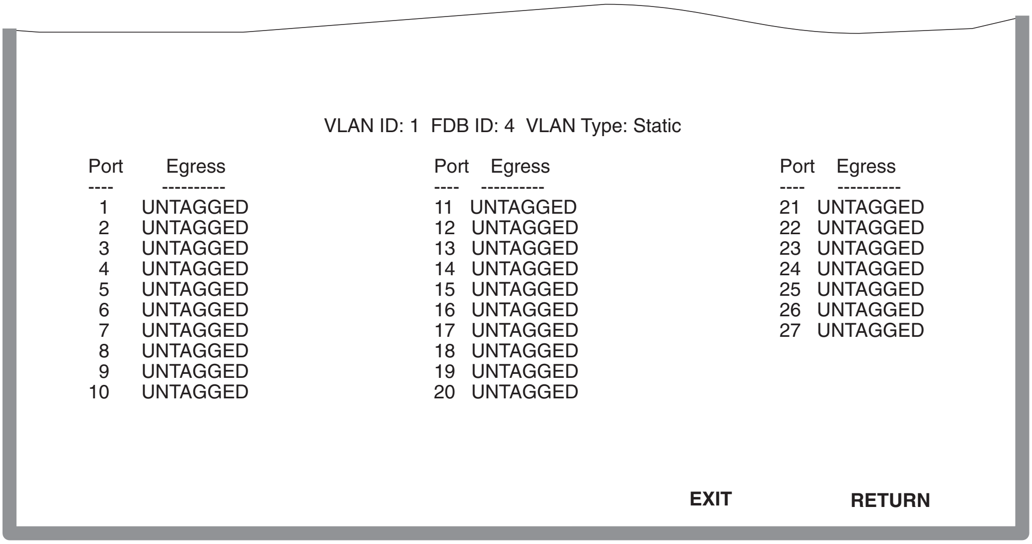
To see the egress settings of all ports associated with the VLAN ID selected from the Current VLAN Configuration screen.

How to Access

Use the arrow keys to highlight the line item with the VLAN ID of interest on the Current VLAN Configuration screen and press ENTER. The Current VLAN Egress Configuration screen, Figure 7-6, displays showing the egress setting of each port associated with the VLAN ID.

Screen Example

Figure 7-6 Current VLAN Egress Configuration Screen



```
                      VLAN ID: 1  FDB ID: 4  VLAN Type: Static

Port     Egress               Port   Egress               Port   Egress
----    ----------            ----  ----------            ----  ----------
  1   UNTAGGED                11  UNTAGGED                21  UNTAGGED
  2   UNTAGGED                12  UNTAGGED                22  UNTAGGED
  3   UNTAGGED                13  UNTAGGED                23  UNTAGGED
  4   UNTAGGED                14  UNTAGGED                24  UNTAGGED
  5   UNTAGGED                15  UNTAGGED                25  UNTAGGED
  6   UNTAGGED                16  UNTAGGED                26  UNTAGGED
  7   UNTAGGED                17  UNTAGGED                27  UNTAGGED
  8   UNTAGGED                18  UNTAGGED
  9   UNTAGGED                19  UNTAGGED
 10   UNTAGGED                20  UNTAGGED
```

30691_36

Field Descriptions

Refer to Table 7-5 for a functional description of each screen field.

Table 7-5 Current VLAN Egress Configuration Screen Field Descriptions

Use this field…	To…
Port (Read-Only)	See a list of the ports associated with the VLAN ID shown in the line above the Port and Egress lists.
Egress (Read-Only)	See the current egress setting (UNTAGGED, TAGGED, or NO) for each port.

7.7 VLAN PORT CONFIGURATION SCREEN

When to Use

To see and/or make changes to the port parameters affecting

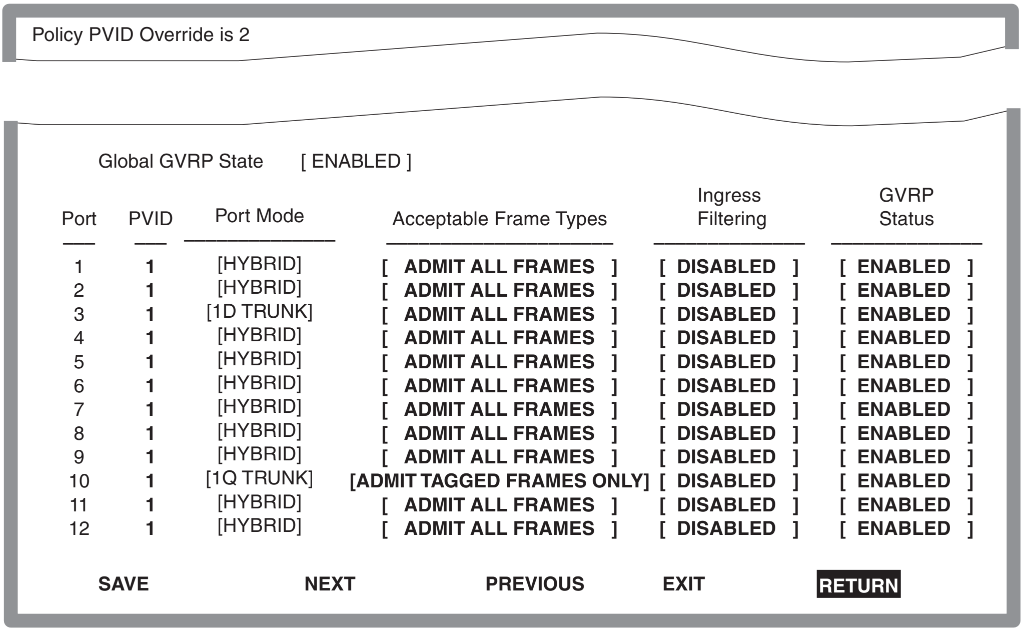
- the Port VLAN Identification (PVID) to reassign the port to a different PVID,
- the acceptable frame type that the port will transmit or receive frames of VLANs other than the static VLANs created on the switch,
- the ingress filtering on the port, which can be enabled or disabled to filter out (drop) frames that are not on the switch Egress list, or
- the GARP VLAN Registration Protocol (GVRP) status, which can be enabled or disabled.

How to Access

Use the arrow keys to highlight the **VLAN PORT CONFIGURATION** menu item on the 802.1Q Configuration Menu screen and press ENTER. The VLAN Port Configuration screen, Figure 7-7, displays.

Screen Example

Figure 7-7 VLAN Port Configuration Screen



```
Policy PVID Override is 2

        Global GVRP State      [ ENABLED ]

                                                        Ingress           GVRP
Port   PVID     Port Mode      Acceptable Frame Types   Filtering         Status
----   ----   -------------   ----------------------   -------------    -------------
 1      1       [HYBRID]       [  ADMIT ALL FRAMES  ]   [ DISABLED ]     [ ENABLED ]
 2      1       [HYBRID]       [  ADMIT ALL FRAMES  ]   [ DISABLED ]     [ ENABLED ]
 3      1     [1D TRUNK]       [  ADMIT ALL FRAMES  ]   [ DISABLED ]     [ ENABLED ]
 4      1       [HYBRID]       [  ADMIT ALL FRAMES  ]   [ DISABLED ]     [ ENABLED ]
 5      1       [HYBRID]       [  ADMIT ALL FRAMES  ]   [ DISABLED ]     [ ENABLED ]
 6      1       [HYBRID]       [  ADMIT ALL FRAMES  ]   [ DISABLED ]     [ ENABLED ]
 7      1       [HYBRID]       [  ADMIT ALL FRAMES  ]   [ DISABLED ]     [ ENABLED ]
 8      1       [HYBRID]       [  ADMIT ALL FRAMES  ]   [ DISABLED ]     [ ENABLED ]
 9      1       [HYBRID]       [  ADMIT ALL FRAMES  ]   [ DISABLED ]     [ ENABLED ]
10      1     [1Q TRUNK]   [ADMIT TAGGED FRAMES ONLY]   [ DISABLED ]     [ ENABLED ]
11      1       [HYBRID]       [  ADMIT ALL FRAMES  ]   [ DISABLED ]     [ ENABLED ]
12      1       [HYBRID]       [  ADMIT ALL FRAMES  ]   [ DISABLED ]     [ ENABLED ]

      SAVE            NEXT           PREVIOUS        EXIT          RETURN
```

36502_05

Field Descriptions

Refer to Table 7-6 for a functional description of each screen field.

Table 7-6 VLAN Port Configuration Screen Field Descriptions

Use this field…	To…
Policy PVID Override is (Read-Only)	See the active override to a port as a result of an application policy. When a port number has an asterisk next to it, selecting that Port field will cause this field to display with the application policy number. There are two sources of an override; 1) default policy, and 2) authentication policy. Authentication using 802.1X is not possible on a port in this mode. In Figure 7-7, the override shown is 2.

Table 7-6 VLAN Port Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Global GVRP State (Toggle)	Enable or Disable the GVRP Status. GVRP and PVST are not interoperable. When ENABLED, GVRP is turned on for the entire switch. When DISABLED, the VLANs are not learned on a given port.
Port (Read-Only)	See a list of the switch ports. **NOTE:** In some cases this field may have an asterisk next to it. It indicates that the port is currently overridden by a policy. If a port with an asterisk is highlighted using the curser, the policy override setting is displayed in the upper left-hand corner of the screen, as shown in Figure 7-7.
PVID (Modifiable)	Change the PVID of one or more ports. The value must be typed in the field. This associates the port to the VLAN associated with the PVID.
Port Mode (Selectable)	See the current operational port mode and select one of the modes: HYBRID, 1Q TRUNK, or 1D TRUNK. The default is HYBRID.
Acceptable Frame Types (Toggle)	Set the port to receive all frames or only tagged frames. The selection can be toggled to either ADMIT ALL FRAMES or ADMIT TAGGED FRAMES ONLY. If a port is to be connected directly to the computer of a user, printer, or other device, set this to ADMIT ALL FRAMES. If a port is going to be used for a trunk port connection to another switch, set this to ADMIT TAGGED FRAMES ONLY.
Ingress Filtering (Toggle)	Enable or disable the ingress filtering on a port. When ENABLED, the device discards incoming frames for VLANs that do not include the selected port in its Member set. When DISABLED, the port will accept all incoming frames. This control does not affect VLAN independent BPDU frames, such as GVRP and STP. It does affect VLAN dependent BPDU frames.
GVRP Status (Toggle)	Enable or disable a port to support dynamic VLANs created by the GARP VLAN Registration Protocol (GVRP). For more information about GVRP, refer to Appendix A.

7.7.1 Changing the Port Mode

To change the operational mode of a port, proceed as follows.

1. Use the arrow keys to highlight the **Port Mode** field for the port you wish to change.
2. Use the SPACE bar or BACKSPACE key to step through the available selections. A port may be configured for any of the following modes:
   - **HYBRID** – This is the default mode for all ports on the switch. The initial Port VLAN List includes the PVID with a frame format of untagged. Any other VLANs desired for the Port VLAN List need to be manually configured. By changing the default mode to 1Q Trunk or 1D Trunk, the Port VLAN List and the associated frame type are automatically configured.
   - **1Q TRUNK** – This mode sets the port for transmitting to another 802.1Q aware device. In this mode, all frames are transmitted with a tag header included in the frame (excluding BPDUs). The switch will drop all untagged frames it receives on the 1Q Trunk port. The Port VLAN List for the port includes all VLANs.
   - **1D TRUNK** – This mode sets the port for transmitting to a legacy 802.1D switch fabric. In this mode, all incoming frames are classified into the default VLAN and all frames are transmitted untagged. The switch expects to receive only untagged frames through the 1D Trunk port. This mode also updates the Port VLAN List and makes the port eligible to transmit frames for all VLANs.
3. When the desired operational mode for the port is displayed, use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

7.7.2 Configuring the VLAN Ports

To configure a VLAN port, proceed as follows:

NOTE: In the following steps, you only need to step to the fields that you are going to change.

1. Use the arrow keys to highlight the **PVID** field.
2. Type the **PVID** number to be assigned to the port.
3. Use the arrow keys to highlight the **Port Mode** field.
4. Press the SPACE bar to select appropriate Port Mode: **HYBRID**, **1Q TRUNK**, or **1D TRUNK**. The default is **HYBRID**.

5. Use the arrow keys to highlight the port’s **Acceptable Frame Types** field.
6. Press the SPACE bar to toggle the field to the correct setting: **ADMIT ALL FRAMES** or **ADMIT TAGGED FRAMES ONLY**.
7. Use the arrow keys to highlight the port’s **Ingress Filtering** field.
8. Press the SPACE bar to toggle the field to the correct setting: **ENABLED** or **DISABLED**. This will either enable or disable the filtering set in the Acceptable Frame Type field in step 5.
9. Use the arrow keys to highlight the port’s **GVRP Status** field.
10. Press the SPACE bar to toggle the field to the correct setting: **ENABLED** or **DISABLED**.
11. To configure more than one port, repeat step 1 through step 10. Then go to step 12 to save your settings.
12. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
13. Press ENTER. The message “SAVED OK” displays and all settings are saved.

7.8 VLAN CLASSIFICATION CONFIGURATION SCREEN

When to Use

To perform the following:

- Display the VLAN ID (VID), Protocol Classification, and Description of each classification of the current entries.
- Assign VLANs according to Classification rules.
- Add/delete a VID and associated classification entry.
- Access the Protocol Port Configuration screen.

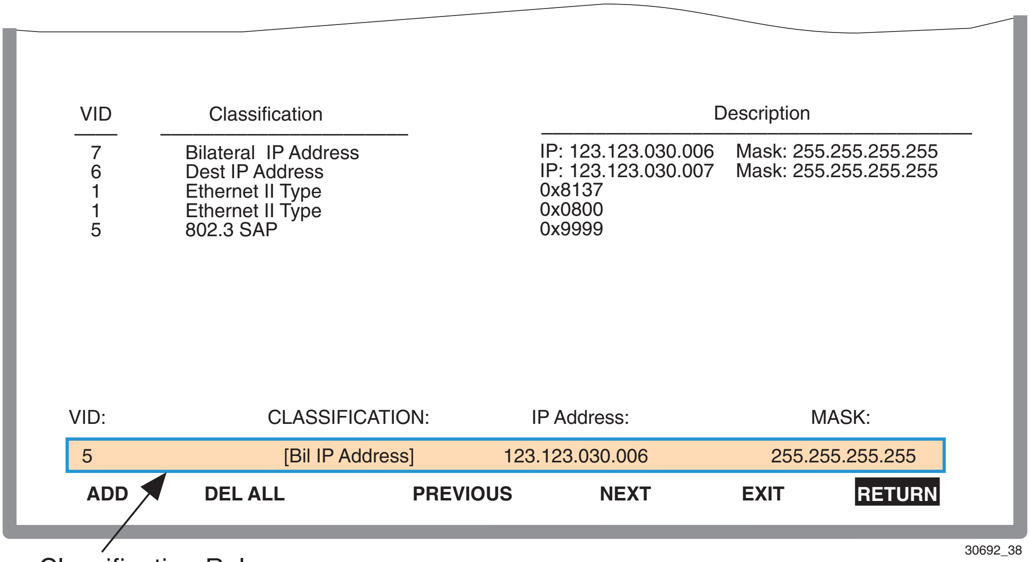
When a frame is received that already contains an 802.1Q frame tag, frame classification is not implemented. Instead, the frame is processed by the SmartSwitch device according to the information contained in the 802.1Q frame tag. When the frame is transmitted, it is sent to the ports associated with the VLAN as established using the Protocol Port Configuration screen described in Section 7.9.

How to Access

Use the arrow keys to highlight the **VLAN CLASSIFICATION CONFIGURATION** menu item on the 802.1Q VLAN Configuration Menu screen and press ENTER. The VLAN Classification Configuration screen, Figure 7-8, displays.

Screen Example

Figure 7-8 VLAN Classification Configuration Screen



```
VID     Classification             Description
7       Bilateral  IP Address      IP: 123.123.030.006   Mask: 255.255.255.255
6       Dest IP Address            IP: 123.123.030.007   Mask: 255.255.255.255
1       Ethernet II Type           0x8137
1       Ethernet II Type           0x0800
5       802.3 SAP                  0x9999

VID:          CLASSIFICATION:        IP Address:            MASK:
5             [Bil IP Address]       123.123.030.006        255.255.255.255
```

Classification Rule

Field Descriptions

Refer to Table 7-7 for a functional description of each screen field.

Table 7-7 VLAN Classification Configuration Screen Field Descriptions

Use this field …	To …
VID – top of screen (Selectable)	See the VLAN Identifications (VIDs) currently associated with a protocol classification. To see which ports are assigned to a VID/Classification, or to add/remove a port from a VID/Classification, use the Protocol Port Configuration screen. For details, refer to Section 7.8.2.

Table 7-7 VLAN Classification Configuration Screen Field Descriptions (Continued)

Use this field …	To …
Classification – top of screen (Selectable)	See the classification associated with the VLAN in the VID column. This field may be selected after the screen is saved to call up the Protocol Port Configuration screen.
Description (Selectable)	See a brief description of the classification.
VID – bottom of screen (Modifiable)	Enter a VLAN Identification (VID) to be associated with the classification selected in the Classification field. For details on how to enter the VID/Classification, refer to Section 7.8.3.
CLASSIFICATION – bottom of screen (Selectable)	Select the classification that will be associated with the VLAN entered in the VID field. There can be up to three fields involved (CLASSIFICATION, IP ADDRESS, and MASK), depending on the classification selected. At the time of this printing, the selections available in each field are listed in Table 7-8. **NOTE:** Besides the VID selected, the order in which a frame is transmitted also depends on the Classification Precedence Rules discussed in Section 7.8.1. These rules come into effect when there are multiple classifications configured in the SmartSwitch device. For details on how to use the VLAN Classification Configuration screen to select the classification rule, refer to Section 7.8.3.
ADD (Command)	Add the current Classification Rule (VID and Classification selections) to the screen. For details about how to add an entry, refer to Section 7.8.3.
DEL ALL/DEL MARKED (Command)	Delete all or one or more marked Classification Rule entries on the screen. The DEL ALL command is the default and it is used to simultaneously delete all the configured Classification Rules. The DEL MARKED command appears in place of the DEL ALL command when one or more lines are marked for deletion. For details on using the two commands, refer to Section 7.8.4.

Table 7-8 provides a list of the Classifications that can be selected in the Classification field and the associated subclassifications.

Table 7-8 Classification List

Classification	Subclassification and Options	Custom or Mask Value
Ethernet II Type>	Ethernet II Type:	
	- IPX	
	- DOD IP	
	- ARP	
	- RARP	
	- AppleTalk	
	- Banyan Vines	
	- DECNET	
	- CUSTOM >	Type Value: 0x**0000**[1]
802.3 SAP>	SSAP/DSAP (802.3):	
Same	- IP	
	- IPX	
	- IPX RAW	
	- BANYAN	
	- SNA	
	- CUSTOM >	DSAP/SSAP Type: 0x**0000**
IP TOS	Type of Service:	
	0x**0000**	

Table 7-8 Classification List (Continued)

Classification	Subclassification and Options	Custom or Mask Value
IP Protocol Type	IP Protocol Type: TCP - UDP - ICMP - IGMP - OSPF - CUSTOM >	Protocol Type: **000**
IPX COS	IPX Class Of Service: **000**	
IPX Packet Type	IPX Packet Type: - Hello or SAP - RIP - Echo Packet - Error Packet - Netware 386/SAP - Seq. Pkt Protocol - Netware 286 - CUSTOM >	IPX Packet Type: **00**
Src IP Address	IP Address: **000.000.000.000**	Mask: **000.000.000.000**
Dest IP Address	IP Address: **000.000.000.000**	Mask: **000.000.000.000**
Bil IP Address	IP Address: **000.000.000.000**	Mask: **000.000.000.000**
Src IPX Network	IPX Network Num: 0x**00000000**	

Table 7-8 Classification List (Continued)

Classification	Subclassification and Options	Custom or Mask Value
Dest IPX Network	IPX Network Num: 0x**00000000**	
Bil IPX Network	IPX Network Num: 0x**00000000**	
Src UDP Port	IP UDP Port: - FTP Data - FTP - BOOTP Server - BOOTP Client - RIP - Telnet - TFTP - HTTP - DNS - SMTP - POP3 - IMAP2 - IMAP3 - NETBIOS Name Serv - NETBIOS Datagram - NETBIOS Sess Serv - CUSTOM >	UDP Port Number: **00000**
Dest UDP Port	IP UDP Port: Same selection as for Src UDP Port Classification	UDP Port Number: **00000**
Bil UDP Port	IP UDP Port: Same selection as for Src UDP Port Classification	UDP Port Number: **00000**

Table 7-8 Classification List (Continued)

Classification	Subclassification and Options	Custom or Mask Value
Src TCP Port	TCP Port: - FTP Data - FTP - BOOTP Server - BOOTP Client - RIP - Telnet - TFTP - HTTP - DNS - SMTP - POP3 - IMAP2 - IMAP3 - NETBIOS Name Serv - NETBIOS Datagram - NETBIOS Sess Serv - CUSTOM >	TCP Port Number: **00000**
Dest TCP Port	TCP Port: Same selection as for Src TCP Port Classification	TCP Port Number: **00000**
Bil TCP Port	TCP Port: Same selection as for Src TCP Port Classification	TCP Port Number: **00000**

Table 7-8 Classification List (Continued)

Classification	Subclassification and Options	Custom or Mask Value
Src IPX Socket	IPX Socket: - NCP - SAP - RIP - NETBIOS - Diagnostics - NLSP - IPX WAN - CUSTOM >	IPX Socket Type: **00000**
Dest IPX Socket	IPX Socket: Same selection as for Src IPX Socket Classification	IPX Socket Type: **00000**
Bil IPX Socket	IPX Socket: Same selection as for Src IPX Socket Classification	IPX Socket Type: **00000**
Src MAC Address	MAC Address: **00-00-00-00-00-00**	
Dest MAC Address	MAC Address: **00-00-00-00-00-00**	
Bil MAC Address	MAC Address: **00-00-00-00-00-00**	
IP Fragments[2]		
Src UDP Range[3]	Start: 00000	End: 00000
Dest UDP Range[3]	Start: 00000	End: 00000
Bil UDP Range[3]	Start: 00000	End: 00000

Table 7-8 Classification List (Continued)

Classification	Subclassification and Options	Custom or Mask Value
Src TCP Range[3]	Start: 00000	End: 00000
Dest TCP Range[3]	Start: 00000	End: 00000
Bil TCP Range[3]	Start: 00000	End: 00000

[1] **Bold** type indicates a user entry.

[2] Any fragmented IP frame received is Classified to the priority identification (PID) and forwarded out the ports configured in the Protocol Port Configuration screen.

[3] This allows the classification of a packet, depending on if the udp/tcp socket falls within the range of the user-entered “Start” and “End” values.

7.8.1 Classification Precedence Rules

NOTE: It is important that you have a comprehensive understanding of the precedence concept before configuring the SmartSwitch device, as these rules can have a significant impact on the network operation.

When there are multiple classifications assigned to a SmartSwitch device, the SmartSwitch device must determine which classification takes precedence according to the Classification Precedence Rules. The order of precedence is predefined in the SmartSwitch device and cannot be changed.

Table 7-9 lists the ISO Layer, associated classification, and precedence levels.

NOTE: In Table 7-9, the following applies:

- Highest precedence is 1a.
- Lowest precedence is 6.
- Exact Match indicates a match of an explicitly defined address.
- Best Match indicates a match of an entire subnet, or range of addresses within a subnet.

Table 7-9 Classification Precedence

Classification Type	Precedence Level
Layer 2	
Source MAC Address Best Match	1a
Destination MAC Address Best Match	1b
EtherType	6
SAP	6
Layer 3	
IP TOS	5a
IP Type	5b
IPX COS	5a
IPX Type	5b
Source IP Address Exact Match	2a
Source IP Address Best Match	2b
Destination IP Address Exact Match	2c
Destination IP Address Best Match	2d
Source IPX Network Number	2a
Destination IPX Network Number	2b
IP Fragments	3

Table 7-9 Classification Precedence (Continued)

Classification Type	Precedence Level
Layer 4	
UDP Port Source	4a
UDP Port Destination	4b
TCP Source Port	4a
TCP Destination Port	4b
IPX Socket Source	4a
IPX Socket Destination	4b
UDP Source Port	4a
UDP Source Port Range	4b
UDP Dest Port	4c
UDP Dest Port Range	4d
TCP Source Port	4a
TCP Source Port Range	4b
TCP Dest Port	4c
TCP Dest Port Range	4d

The following example shows how the precedence concept can be applied:

Example

A network administrator has defined the following two classifications involving VLANs:

- All frames with a UDP Port Source number of 55 (Layer 4, precedence level 4a) are assigned to the Red VLAN.
- All frames sourced from the 134.141.28.xx subnet (Layer 3, Source IP Address Best Match, level 2b) are assigned to the Blue VLAN.

In this example, a frame that is received with a source address of 134.141.28.99 and contains a UDP port number of 55 will be assigned to the Blue VLAN because a Layer 3 IP Address rule takes precedence over a Layer 4 rule.

The key thing to remember is that the SmartSwitch devices will classify frames based on one of the classification options.

7.8.2 Displaying the Current Classification Rule Assignments

To see which ports are set to a particular Classification Rule, the Protocol Port Configuration screen must be displayed.

To access the Protocol Port Configuration, proceed as follows:

1. Use the arrow keys to highlight the **line** with the Classification Rule of interest.
2. Press ENTER. The Protocol Port Configuration screen displays, showing all ports and those associated with the Classification Rule selected in step 1. These ports are identified on the screen by a **YES** setting in the Classify columns. For more information about the Protocol Port Configuration screen and how to use it, refer to Section 7.9.

7.8.3 Assigning a Classification to a VID

NOTE: It is strongly recommended that you read Section 7.8.1 for more information concerning classification before configuring the SmartSwitch device. Incorrect configuration will affect network operation.

To assign a Classification to a VID, proceed as follows:

1. Use the arrow keys to highlight the **VID** (VLAN identification) field.
2. Type in the appropriate VID. Press ENTER.
3. Use the arrow keys to highlight the **Classification** field.
4. Press the SPACE bar to step to the appropriate Classification. Table 7-8 lists the subclassification associated with each Classification (examples of classifications: Ethernet II Type, 802.3 SAP, IP TOS, IP Protocol Type, etc.).
5. Use the arrow keys to highlight the subclassification field to the immediate right of the Classification field. The name of the field changes depending on the selected Classification, as shown in Table 7-8 (examples of subclassification: Ethernet II Type, SSAP/DSAP (802.3), Type of Service, IP Protocol Type, etc.).
6. Press the SPACE bar to step to the appropriate protocol. In some cases, there is only one selection and a value needs to be entered. This is indicated by **bold** zeros. Table 7-8 lists the possible selections associated with each subclassification (examples: IPX, AppleTalk, NetBIOS, Banyan Vines, **000.000.000.000**, 0x**00000000**, etc.).
7. In some cases, a selection in the subclassification field requires a value to be entered in a third field to the right of the subclassification field. If so, use the arrow keys to highlight that third field and type in the appropriate value. Otherwise, go to step 8.
8. Use the arrow keys to highlight the **ADD** command field.
9. Press ENTER to save the VID and Classification settings. After a brief delay, the Classification Rule will display in the top half of the screen.

NOTE: After creating a classification rule you must assign it to the appropriate ports using the Protocol Port Configuration screen described in Section 7.9.

7.8.4 Deleting Line Items

All, or one or more, line items can be deleted as follows:

Deleting All Classification Rules

To delete all the Classification Rules in the top half of the screen, use the arrow keys to highlight the **DEL ALL** command field and press ENTER.

Deleting One or More Classification Rules

To delete one or more Classification Rules, mark each one and then delete them, as follows:

1. Use the arrow keys to highlight the line with the **Classification Rule** to be deleted.
2. Press the **M** key and an asterisk (*) appears next to the highlighted line to mark it. The DEL ALL command is changed to DEL MARKED.
3. If more than one Classification Rule is to be deleted, repeat steps 1 and 2 to mark each line.

NOTE: If for some reason you want to remove a mark, perform steps 1 and 2. Pressing the **M** key when a marked line is highlighted will remove the mark. If all marks are removed, the DEL MARKED command is changed back to DEL ALL.

4. After the lines are marked, use the arrow keys to highlight the **DEL MARKED** command field.
5. Press ENTER. The marked line items are deleted and the DEL MARKED command is changed back to DEL ALL.

7.9 PROTOCOL PORT CONFIGURATION SCREEN

When to Use

To perform the following:

- Display the ports.
- Show which ports are set to the line item containing the VID/Classification (Classification Rule) of interest in the VLAN Classification Configuration screen described in Section 7.8.
- Add or remove ports from being associated with the Classification Rule.

- Add ports to the VLAN Forwarding List of the SmartSwitch device.

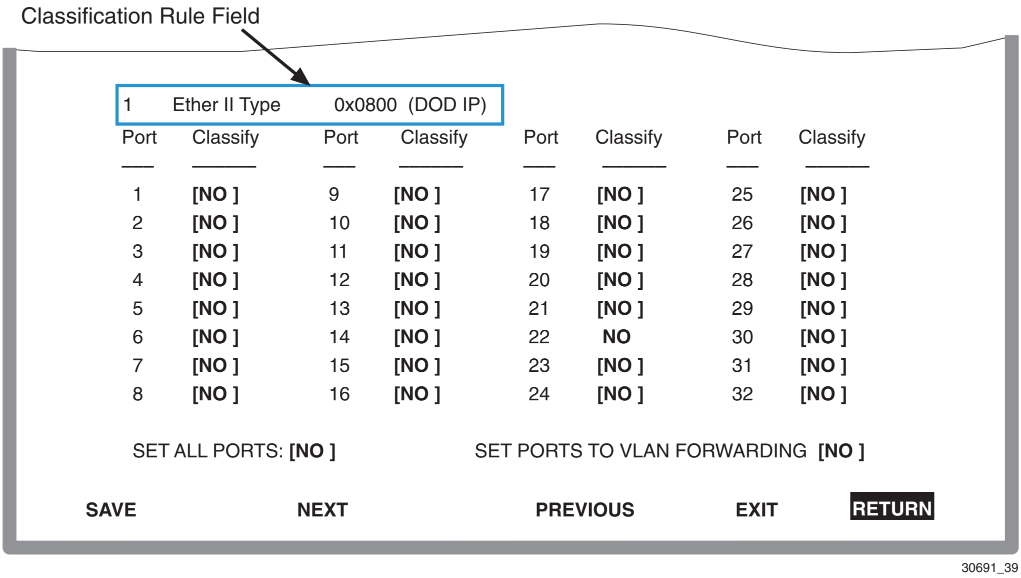
NOTE: The ports can only be added to the VLAN Forwarding List of an existing VLAN. If the VLAN does not exist, it must be created before the ports can be assigned to the VLAN Forwarding List. VLANs are created using the Static VLAN Configuration screen described in Section 7.3.

How to Access

Use the arrow keys to highlight the line item of interest on the VLAN Classification Configuration screen and press ENTER. The Protocol Port Configuration screen (Figure 7-9) displays.

Screen Example

Figure 7-9 Protocol Port Configuration Screen



```
1     Ether II Type        0x0800  (DOD IP)
Port    Classify       Port    Classify       Port    Classify       Port    Classify
____    ________       ____    ________       ____    ________       ____    ________

 1      [NO ]           9      [NO ]          17      [NO ]          25      [NO ]
 2      [NO ]          10      [NO ]          18      [NO ]          26      [NO ]
 3      [NO ]          11      [NO ]          19      [NO ]          27      [NO ]
 4      [NO ]          12      [NO ]          20      [NO ]          28      [NO ]
 5      [NO ]          13      [NO ]          21      [NO ]          29      [NO ]
 6      [NO ]          14      [NO ]          22       NO            30      [NO ]
 7      [NO ]          15      [NO ]          23      [NO ]          31      [NO ]
 8      [NO ]          16      [NO ]          24      [NO ]          32      [NO ]

    SET ALL PORTS: [NO ]               SET PORTS TO VLAN FORWARDING  [NO ]

SAVE              NEXT                PREVIOUS          EXIT        RETURN
```

Field Descriptions

Refer to Table 7-10 for a functional description of each screen field.

Table 7-10 Protocol Port Configuration Screen Field Descriptions

Use this field …	To …
Classification Rule Field (Read-Only)	See the VID, Classification, and Definition of the line selected in the VLAN Classification Configuration screen. For example, in Figure 7-9, VID 1, Ether II Type, 0x0800 (DOD IP) was selected in the VLAN Classification Configuration screen to access the Protocol Port Configuration screen. All ports with YES in the Classify columns indicate that they are associated with VID 1 and the Ether II Type Classification. This causes the VLAN 1, Ether II Type frames that are received to be classified into VID 1. This will cause Ether II of type 0x0800 (DOD IP) frames to be transmitted out all ports set to YES as frames belonging to VLAN 1.
Port (Read-Only)	See the number of each port.
Classify (Toggle)	See which ports are set to the VID/Classification displayed in the Classification Rule field above the Port and Classify column headings. This field toggles between YES and NO, which determines whether or not the associated port is set to the VID/Classification indicated in the Classification Rule field. **NOTE:** As each Classify field is highlighted, the Event Message Line (not shown) at the top of the screen indicates the port type. For example: Fast Ethernet Front Panel, FTM Backplane Port 3, and Gigabit Ethernet VHSIM. If a port cannot be configured, NO will be displayed without brackets. In some cases the Classify field [NO] may have an asterisk next to it. The asterisk indicates this classification rule is active as a result of application by policy.
SET ALL PORTS (Toggle)	Set all ports to the VLAN and Classification shown in the Classification Rule field. The SET ALL PORTS field toggles between NO and YES with NO as the default setting. YES associates all ports set to YES to the VID/Classification shown in the Classification Rule field.

Table 7-10 Protocol Port Configuration Screen Field Descriptions (Continued)

Use this field …	To …
SET PORTS TO VLAN FORWARDING (Toggle)	Add the VLAN and classification shown in the Classification Rule field to the Port VLAN List of all ports set to YES. The SET PORTS TO VLAN FORWARDING field toggles between NO and YES with NO as the default setting. YES adds all the ports set to YES to the VLAN Forwarding list of the SmartSwitch device.

7.9.1 Assigning Ports to a VID/Classification

The following procedures describe how to

- assign one or more ports to a Classification Rule,
- set all ports simultaneously to a Classification Rule, or
- enable all selected ports to forward frames with the Classification Rule by adding that Classification Rule to the Port VLAN List of each port.

Assigning One or More Ports Individually

1. Use the arrow keys to highlight the **Classify** field adjacent to the Port number.
2. Press the SPACE bar to toggle the Classify field to **YES** or **NO**. YES assigns the port to the VID/Classification shown in the Classification Rule field. NO removes the port from the Classification Rule.
3. If more than one port is to be added to the Classification Rule, repeat the first two steps for each port.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
5. Press ENTER. The message “SAVED OK” displays and the settings are saved.

Assigning All Ports Simultaneously

1. Use the arrow keys to highlight the **SET ALL PORTS** command field.
2. Press the SPACE bar to toggle the SET ALL PORTS field to **YES** or **NO** and press ENTER. YES will set all the ports to the VID/Classification shown in the Classification Rule field. NO will remove all ports from the Classification Rule.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays and the setting is saved.

Assigning VID/Classification to Port VLAN Lists

1. Use the arrow keys to highlight the **SET PORTS TO VLAN FORWARDING** command field.
2. Press the SPACE bar to toggle the SET PORTS TO VLAN FORWARDING command field to **YES** or **NO**. Press ENTER.

   YES will add the Classification Rule to the Port VLAN List of each port that has been set to YES using one of the two procedures previously described. NO will remove the Classification Rule from all the ports selected.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message "SAVED OK" displays and the setting is saved.

8

802.1p Configuration Menu Screens

This chapter describes the 802.1p Configuration Menu screen and the following screens that may be selected from its menu:

- Port Priority Configuration screen (Section 8.2)
- Traffic Class Information screen (Section 8.3)
  - Traffic Class Configuration screen (Section 8.4)
- Transmit Queues Configuration screen (Section 8.5)
- Priority Classification Configuration screen (Section 8.6)
  - Protocol Port Configuration screen (Section 8.7)
- Rate Limiting Configuration screen (Section 8.8)

Screen Navigation Paths

Password > Device Menu > Device Configuration Menu > 802.1 Configuration Menu > **802.1p Configuration Menu**

8.1 802.1p CONFIGURATION MENU SCREEN

When to Use

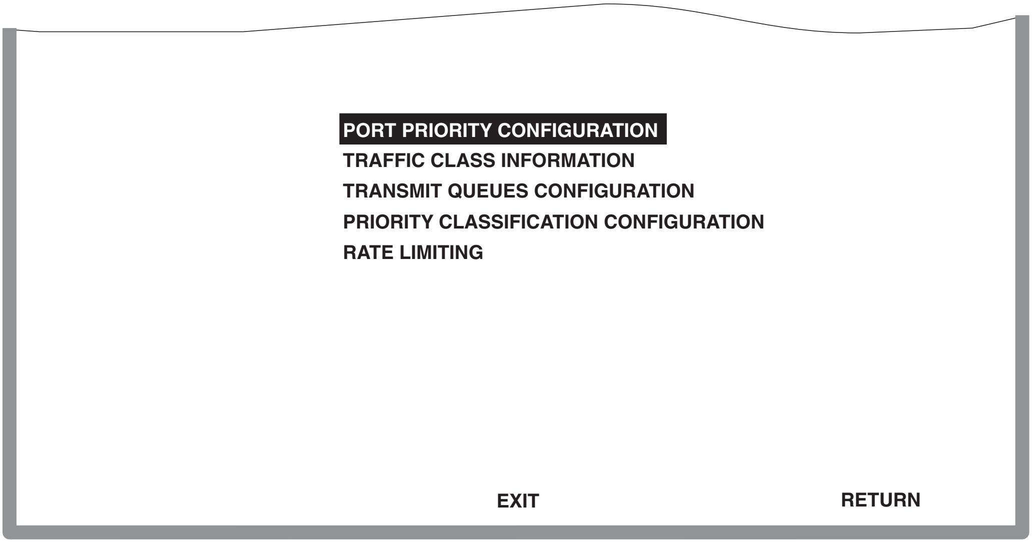
To select the screens used for setting port priority, priority classifications, or configuring rate limiting.

How to Access

Use the arrow keys to highlight the **802.1p CONFIGURATION MENU** item on the 802.1 Configuration Menu screen and press ENTER. The 802.1p Configuration Menu screen, Figure 8-1, displays.

Screen Example

Figure 8-1 802.1p Configuration Menu Screen


PORT PRIORITY CONFIGURATION
TRAFFIC CLASS INFORMATION
TRANSMIT QUEUES CONFIGURATION
PRIORITY CLASSIFICATION CONFIGURATION
RATE LIMITING
EXIT
RETURN

3650-011_06

Menu Descriptions

Refer to Table 8-1 for a functional description of each menu item.

Table 8-1 802.1p Configuration Menu Screen Menu Item Descriptions

Menu Item	Screen Function
PORT PRIORITY CONFIGURATION	Used to view or change the port default transmit priority (0 through 7) of each port for frames that are received (ingress) without priority information in their tag header. For additional information, refer to Section 8.2.
TRAFFIC CLASS INFORMATION	Used to display the current traffic class mapping-to-priority of each port. For details, refer to Section 8.3. This screen is also used to select a port to display the Traffic Class Configuration screen, where the current setting for that port or all ports may be changed simultaneously. For details, refer to Section 8.4.
TRANSMIT QUEUES CONFIGURATION	Used to set each port individually, or all ports simultaneously, to either transmit frames according to the priority transmit queues set in the Advanced Port Priority Configuration screen, or transmit frames according to a priority based on a percentage of port transmission capacity for each transmit queue. For details, refer to Section 8.5.
PRIORITY CLASSIFICATION CONFIGURATION	Used to assign transmit priorities to protocol types of received frames. For details, refer to Section 8.6. This screen is also used to access the Protocol Port Configuration screen to add or delete transmitting ports associated with a specific priority. For details about the Protocol Port Configuration screen, refer to Section 8.7.
RATE LIMITING	Used to configure a rate limit for a given port and list of priorities. This is a traffic rate policing feature used to control the rate of traffic on a per port/priority basis. The list of priorities can include one, some, or all of the eight 802.1p priority levels. For details, refer to Section 8.8.

8.2 PORT PRIORITY CONFIGURATION SCREEN

When to Use

To set the priority (0 through 7) on each port. A port receiving a frame without priority information in its tag header is assigned a priority according to the priority setting on the port. For example, if the priority of a port is set to 5, the frames received through that port without a priority indicated in their tag header are classified as a priority 5.

A frame with priority information in its tag header is transmitted according to that priority.

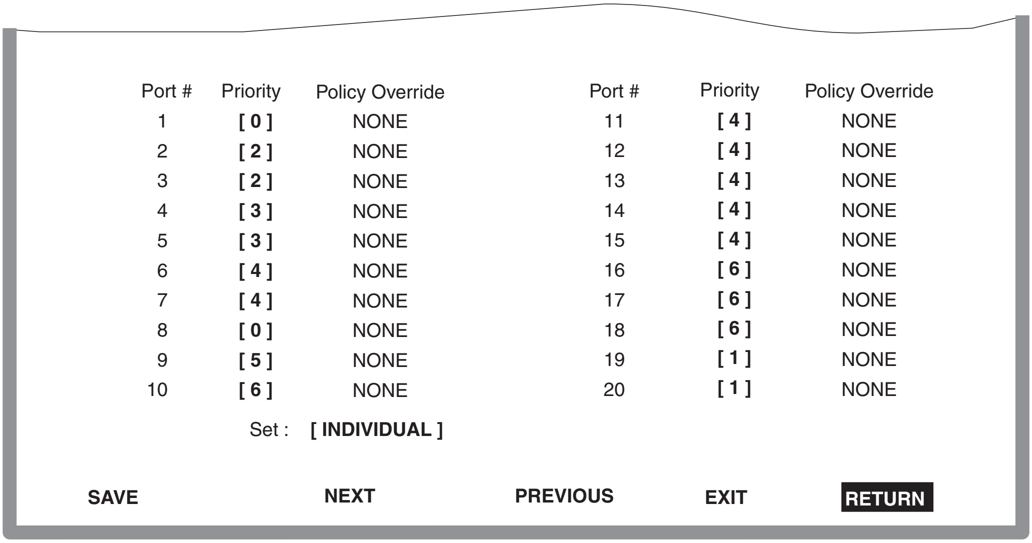
NOTE: The priority is only changed while the SmartSwitch device is processing the frame. Frames received by the SmartSwitch device with a 1p priority value are transmitted with that same value.

How to Access

Use the arrow keys to highlight the **PORT PRIORITY CONFIGURATION** menu item on the 802.1p Configuration Menu screen and press ENTER. The Port Priority Configuration screen, Figure 8-2, displays.

Screen Example

Figure 8-2 Port Priority Configuration Screen

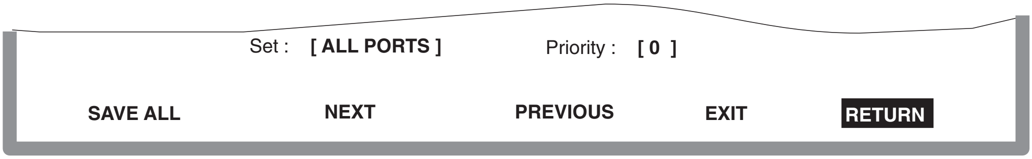


```
Port #  Priority  Policy Override        Port #  Priority  Policy Override
  1      [ 0 ]        NONE                 11     [ 4 ]        NONE
  2      [ 2 ]        NONE                 12     [ 4 ]        NONE
  3      [ 2 ]        NONE                 13     [ 4 ]        NONE
  4      [ 3 ]        NONE                 14     [ 4 ]        NONE
  5      [ 3 ]        NONE                 15     [ 4 ]        NONE
  6      [ 4 ]        NONE                 16     [ 6 ]        NONE
  7      [ 4 ]        NONE                 17     [ 6 ]        NONE
  8      [ 0 ]        NONE                 18     [ 6 ]        NONE
  9      [ 5 ]        NONE                 19     [ 1 ]        NONE
 10      [ 6 ]        NONE                 20     [ 1 ]        NONE

              Set :  [ INDIVIDUAL ]

SAVE            NEXT          PREVIOUS        EXIT        RETURN
```

NOTE: The Set field toggles from INDIVIDUAL to ALL PORTS. When ALL PORTS is selected, the Priority field displays to the right of the Set field and the SAVE command changes to SAVE ALL as shown below.



```
              Set :  [ ALL PORTS ]          Priority :  [ 0 ]

SAVE ALL        NEXT          PREVIOUS        EXIT        RETURN
```

3650-011_41

Field Descriptions

Refer to Table 8-2 for a functional description of each screen field.

Table 8-2 Port Priority Configuration Screen Field Descriptions

Use this field…	To…
Port # (Read-Only)	See the port number. Up to 10 rows of port numbers can be displayed per screen with a maximum of 4 columns. The list of ports can include both physical and virtual ports. If the number of ports exceed these limits, one or more other screens may be accessed using the NEXT and PREVIOUS commands.
Priority (Selectable)	Select a default priority from 0 to 7 for each port. When the screen is displayed the current default priority settings are shown for each port. For details, refer to Section 8.2.1.
Policy Override (Read-Only)	View any active policy override.
Set (Toggle)	Set the priority for one port or set all the ports to the same priority. This field toggles between INDIVIDUAL and ALL PORTS. INDIVIDUAL is the default setting. When set to INDIVIDUAL, the priority of various ports may be changed individually and saved. When set to ALL PORTS, a Priority field displays to the right of the Set field, and the SAVE command changes to SAVE ALL. This allows you to select one priority and apply it to all ports. For details, refer to Section 8.2.2.

8.2.1 Setting Switch Port Priority Port-by-Port

To set the default port priority on a particular port, proceed as follows:

1. Use the arrow keys to highlight the **Set** field.
2. Press the SPACE bar to step to the **INDIVIDUAL** setting.
3. Use the arrow keys to highlight the **Priority** field for the particular port.
4. Press the SPACE bar to step to the appropriate value: **0** through **7**.
5. If more than one port is to be changed, repeat steps 3 and 4 to change the setting for each port, then perform step 6 to save all the changes.
6. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
7. Press ENTER. The message “SAVED OK” displays and the setting is saved.

8.2.2 Setting Switch Port Priority on All Ports

To set the port priority on all ports simultaneously, proceed as follows:

1. Use the arrow keys to highlight the **Set** field.
2. Press the SPACE bar to step to the **ALL PORTS** setting. A Priority field displays to the right of the Set field.
3. Use the arrow keys to highlight the **Priority** field.
4. Press the SPACE bar to select a priority from **0** through **7** (0 is the lowest priority).
5. Use the arrow keys to highlight the **SAVE ALL** command at the bottom of the screen.
6. Press ENTER. The message “SAVED OK” displays and all ports are set to the priority selected in step 4 and saved.

8.3 TRAFFIC CLASS INFORMATION SCREEN

When to Use

To view the current mapping of the Traffic Class-to-priority for each port, which can include both physical and virtual ports. If the number of ports exceeds 12 ports, then other ports can be displayed using the NEXT command.

With this screen, you can also select a port and access the Traffic Class Configuration screen, which allows you to change the Traffic Class (0 -3, with 0 being the lowest level) for each priority of the selected port. Then you can apply the new settings to either the selected port or to all the ports.

NOTE: The priority is only changed while the SmartSwitch device is processing the frame. Frames received by the SmartSwitch device with a 1p priority value are transmitted with that same value.

Priority-to-Traffic Class Mapping is used to assign 802.1p priority values to a Traffic Class (0 through 3 with 0 being the lowest level Traffic Class) for each frame priority.

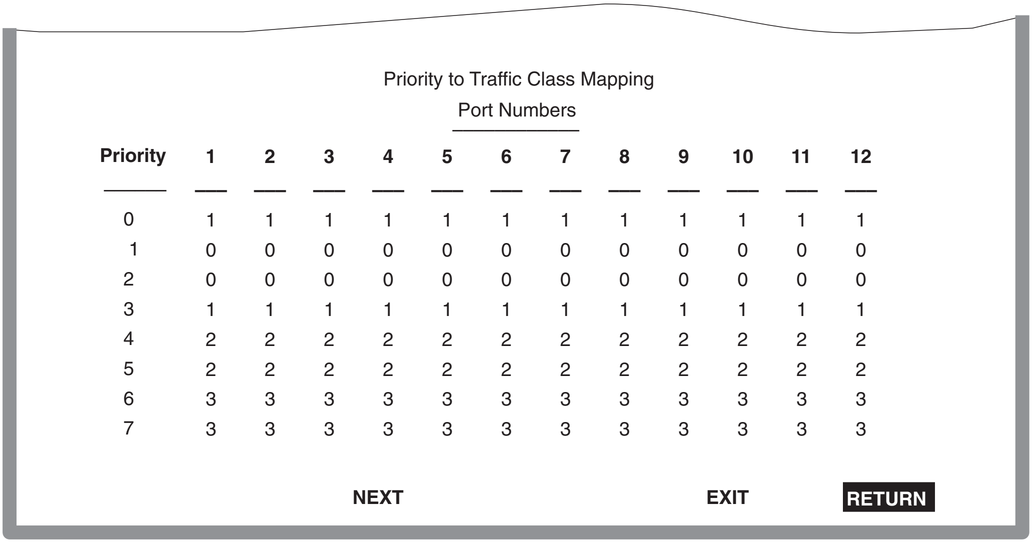
For example, if the Traffic Class is set to 3 for those frames with a priority 7, then those frames would be transmitted before any frames contained in Traffic Classes 2 through 0.

How to Access

Use the arrow keys to highlight the **TRAFFIC CLASS INFORMATION** menu item on the 802.1p Configuration Menu screen and press ENTER. The Traffic Class Information screen, Figure 8-3, displays.

Screen Example

Figure 8-3 Traffic Class Information Screen



Priority to Traffic Class Mapping

Port Numbers

Priority	1	2	3	4	5	6	7	8	9	10	11	12
0	1	1	1	1	1	1	1	1	1	1	1	1
1	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0
3	1	1	1	1	1	1	1	1	1	1	1	1
4	2	2	2	2	2	2	2	2	2	2	2	2
5	2	2	2	2	2	2	2	2	2	2	2	2
6	3	3	3	3	3	3	3	3	3	3	3	3
7	3	3	3	3	3	3	3	3	3	3	3	3

30692_42

Field Descriptions

Refer to Table 8-3 for a functional description of each screen field.

Table 8-3 Traffic Class Information Screen Field Descriptions

Use this field…	To…
Priority (Read-Only)	View eight priority levels of a port that can be associated with Traffic Class settings. When the screen is displayed the current default Traffic Class-to-priority settings are shown for each port. This screen is also used to select a port to display its Traffic Class Configuration screen, where the current setting for that port or all ports may be changed simultaneously. The Traffic Class Configuration screen is described in Section 8.4.
Port (Read-Only)	View up to 12 port numbers along with their Traffic Class-to-priority settings. If the number of ports on the SmartSwitch device exceed 12, one or more screens may be viewed using the NEXT and PREVIOUS commands. The port fields can also be used to access its Traffic Class Configuration screen, where the current Traffic Class-to-priority settings may be changed and applied to that port only or to all ports. For details, refer to **How to Access** in Section 8.4.

8.4 TRAFFIC CLASS CONFIGURATION SCREEN

When to Use

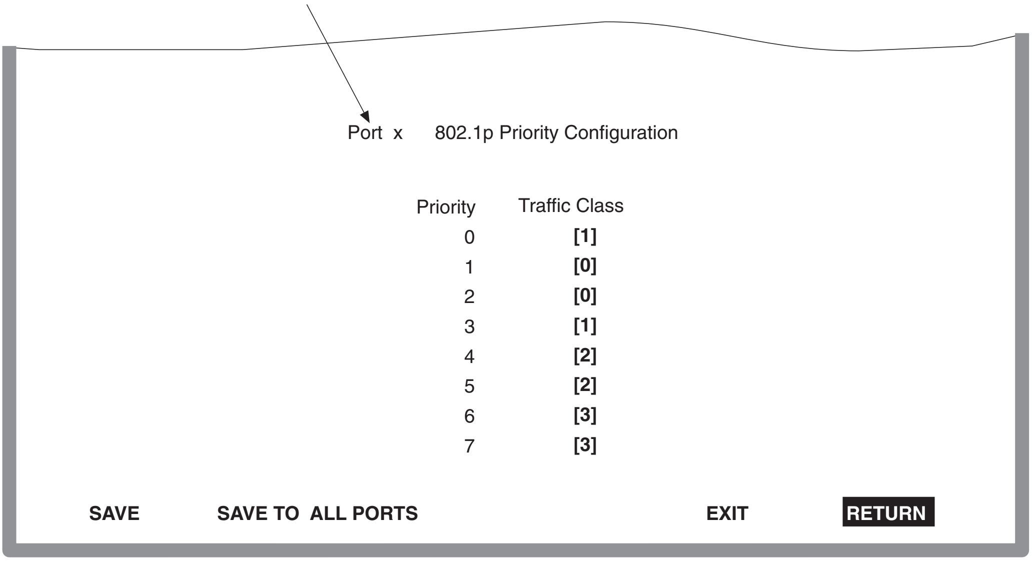
To change the Traffic Class setting of one or more priorities on each port. The new Traffic Class settings may be applied only to the port selected or to all ports, simultaneously.

How to Access

Use the arrow keys to highlight the appropriate **port number** field above the column of the Traffic Class settings in the Traffic Class Information screen. Press ENTER. The Traffic Class Configuration screen, Figure 8-4, for the selected port is displayed, showing its current Traffic Class assignment for each Port Priority.

Screen Example

Figure 8-4 Traffic Class Configuration Screen



Number of port selected in the Traffic Class Information screen.

```
                    Port  x     802.1p Priority Configuration


                          Priority      Traffic Class
                              0              [1]
                              1              [0]
                              2              [0]
                              3              [1]
                              4              [2]
                              5              [2]
                              6              [3]
                              7              [3]

   SAVE        SAVE TO  ALL PORTS                       EXIT        RETURN
```

30691_43

Field Descriptions

Refer to Table 8-4 for a functional description of each screen field.

Table 8-4 Traffic Class Configuration Screen Field Descriptions

Use this field…	To…
Priority (Read-Only)	See the list of eight priority levels (0 through 7) that can be associated with the Traffic Class settings. Priority 0 is the lowest priority. When the screen is displayed, the current default Traffic Class-to-priority settings are shown for the selected port.
Traffic Class (Selectable)	Enable the frames with a certain priority to be mapped to transmit according to one of four Traffic Classes (0 through 3) with 0 being the lowest transmit level. Refer to the following table for the Traffic Class default values according to port priority. **Port Priority**: 0, 1, 2, 3, 4, 5, 6, 7 **Traffic Class**: 1, 0, 0, 1, 2, 2, 3, 3 For details on how to set the Traffic Class for each priority, refer to Section 8.4.1.
SAVE (Command)	Save the Traffic Class selections for each priority and apply them only to the selected port.
SAVE TO ALL PORTS (Command)	Save the Traffic Class selections for each priority and apply them to all ports.

Port Priority	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Traffic Class	1	0	0	1	2	2	3	3

8.4.1 Assigning the Traffic Class to Port Priority

To map the Traffic Class to Priority and apply it to either the selected port only or to all front panel Ethernet ports, proceed as follows:

1. Use the arrow keys to highlight the **Traffic Class** field next to the appropriate priority in the Priority list.
2. Press the SPACE bar to step to the appropriate value, **0** through **3**. The 0 selection is the lowest level Traffic Class setting.
3. If more than one Traffic Class setting is to be changed, repeat steps 1 and 2 until all of the changes in the Traffic Class settings have been made.

4. To save and apply the settings to only the port shown on the screen, proceed to step 5. To save the Traffic Class selections and apply them to all front panel Ethernet ports, proceed to step 6.
5. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER. The message “SAVED OK” displays and the settings are saved.
6. Use the arrow keys to highlight the **SAVE TO ALL PORTS** command at the bottom of the screen and press ENTER. The message “SAVED OK” displays and the settings are saved.

8.5 TRANSMIT QUEUES CONFIGURATION SCREEN

When to Use

To configure the operational mode of the transmit queues to either STRICT 802.1 or WEIGHTED. This enables individual ports or all ports to be set to either transmit frames according to the priority transmit queues set in the Advanced Priority Configuration screen, or transmit frames according to a priority based on a percentage of the port transmission capacity allocated for each transmit queue.

In the STRICT 802.1 mode, frames are transmitted strictly according to the priorities set in the Advanced Priority Configuration screen. In this mode all frames with a transmit queue of Q3 are transmitted first, followed by those with transmit queue of Q2, then Q1, and finally Q0.

In the WEIGHTED mode, a percentage (weighted value) is user assigned to establish the amount of transmission capacity assigned to frames associated with each priority transmit queue (Q0 through Q3 with Q0 being the lowest priority transmit queue). This allows the modification of the strict priority queues so that frames with the lower priority queue are guaranteed some access time to the transmitter.

For example, the transmit queues could be set as follows:

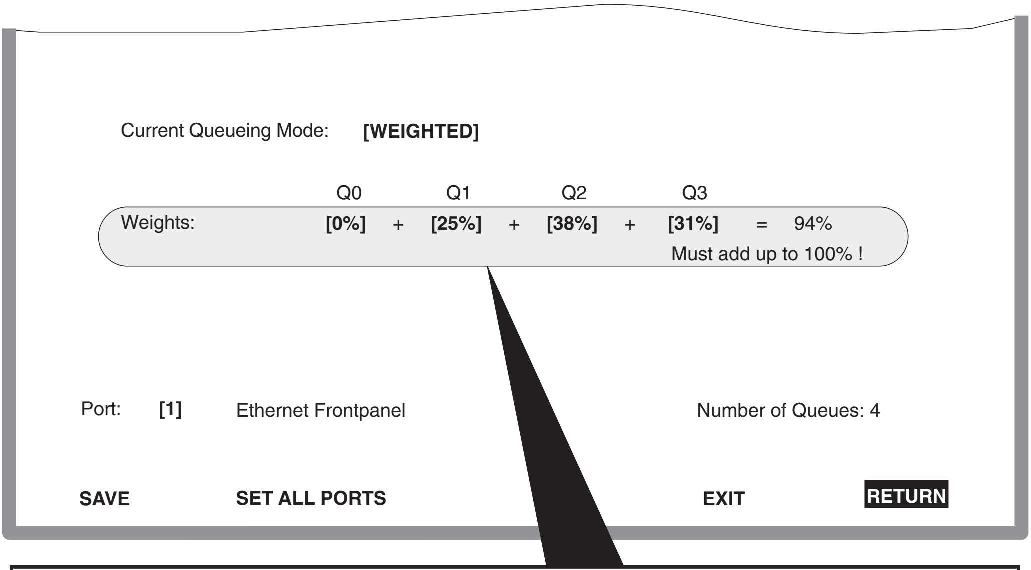
- Q3 to 50%, so at least 50% of the Q3 frames are transmitted.
- Q2 to 25%, so at least 25% of the Q2 frames are transmitted.
- Q1 to 25%, so at least 25% of the Q1 frames are transmitted.
- Q0 to 0%, no Q0 frames will be transmitted until Q3, Q2, and Q1 frames are transmitted.

How to Access

Use the arrow keys to highlight the **TRANSMIT QUEUES CONFIGURATION** menu item on the 802.1p Configuration Menu screen and press ENTER. The Transmit Queues Configuration screen, Figure 8-5, displays.

Screen Example

Figure 8-5 Transmit Queues Configuration Screen



```
          Current Queueing Mode:    [WEIGHTED]

                                Q0        Q1        Q2        Q3
          Weights:             [0%]  +  [25%]  +  [38%]  +  [31%]   =   94%
                                                            Must add up to 100% !

      Port:   [1]      Ethernet Frontpanel                  Number of Queues: 4

      SAVE             SET ALL PORTS                        EXIT          RETURN
```

These fields display only when the Current Queueing Mode is set to **WEIGHTED**. The "Must add up to 100%!" message displays as long as the total percentage is not 100%, as shown.

30691_45

Field Descriptions

Refer to Table 8-5 for a functional description of each screen field.

Table 8-5 Transmit Queues Configuration Screen Field Descriptions

Use this field …	To…
Current Queueing Mode (Toggle)	Toggle between the STRICT 802.1 and WEIGHTED mode. The default setting is STRICT 802.1. To set the mode, refer to Section 8.5.1.
Weights Q0, Q1, Q2, Q3 (Selectable)	Allocate the percentage of port transmission capacity according to transmit queues Q0 through Q3 (with Q0 being the lowest priority transmit queue). **NOTE:** These selectable fields (Q0 through Q3) do not display when the Current Queueing Mode is set to STRICT 802.1. The weights selected must equal 100% or the values cannot be saved. Default weight distribution is 25% per transmission queue. Selectable percent weight values per priority transmit queue Q0 through Q3 are as follows: 00, 06, 12, 19, 25, 31, 38, 44, 50, 56, 62, 69, 75, 81, 88, 94, 100. To set the weight per priority, refer to Section 8.5.1.
Port (Selectable)	Step to the port to be configured. As each port is stepped to, the port type (e.g., Ethernet front panel) displays to the right of the selected port number. To display the current weight settings for the selected port, press ENTER.
Number of Queues (Read-Only)	See the number of Queues.
SET ALL PORTS (Command)	Set all available ports to the current screen settings. **NOTE:** These selectable fields (Q0 through Q3) do not display when the Current Queueing Mode is set to STRICT 802.1.

8.5.1 Setting the Current Queueing Mode

To set the current queueing mode for a particular port, proceed as follows:

1. Use the arrow keys to highlight the **Port** field.
2. Press the SPACE bar to step to the appropriate port number. The port type displays to the right of the Port number field.

TIP: To display the current port settings, press ENTER after selecting the port number.

3. Use the arrow keys to highlight the **Current Queueing Mode** field.
4. To select the Current Queueing Mode for the port selected in step 1, press the SPACE bar to toggle to either **STRICT 802.1** or **WEIGHTED**. The default is STRICT 802.1.

   If STRICT 802.1 is selected, the frames will be transmitted out the selected port according to the frame transmit priority queue set in the Advanced Priority Configuration screen. The weight priority transmit queue fields, Q0 through Q3, do not display. Go to step 8 to save the setting.

   If WEIGHTED is selected, the weight priority transmit queue fields, Q0 through Q3, display. The frames will be transmitted out the port according to the percent of transmit capacity allocated for each transmit queue. The default percentages are 25% for each transmit queue (Q0 through Q3). To set the priority transmit queue fields, go to step 5.
5. Use the arrow keys to highlight the **Q0** field.
6. Use the SPACE bar to step to the appropriate percent value for the priority transmit queue, Q0. Q0 is the lowest priority transmit queue. Repeat this step for Q1, Q2, and Q3.

NOTE: Total percentage of transmit queues Q0 through Q3 must add up to 100% or the values cannot be saved.

For example: Q0, 0%+ Q1, 25% + Q2, 25% + Q3, 50% = 100%

7. To save the settings so they apply to the port selected in step 1, go to step 8. To save the settings so they apply to all available ports, proceed to step 9.
8. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen. Then press ENTER. The message “SAVED OK” displays and the settings are saved for the port selected in step 1.
9. Use the arrow keys to highlight the **SET ALL PORTS** command. Then press ENTER. The message “SAVED OK” displays and the settings are saved for available ports.

8.6 PRIORITY CLASSIFICATION CONFIGURATION SCREEN

When to Use

To perform the following functions:

- Display the current Priority, Classification, and Description entries of each classification rule.
- Assign priorities according to Classification Rules.
- Add/delete a priority and associated protocol entry.
- Access the Protocol Port Configuration screen.
- Assign an 8-bit TOS (also known as DF) value to incoming IP frames. For more information on the IP TOS Function, refer to Section 8.6.2.
- Write over an existing TOS value.

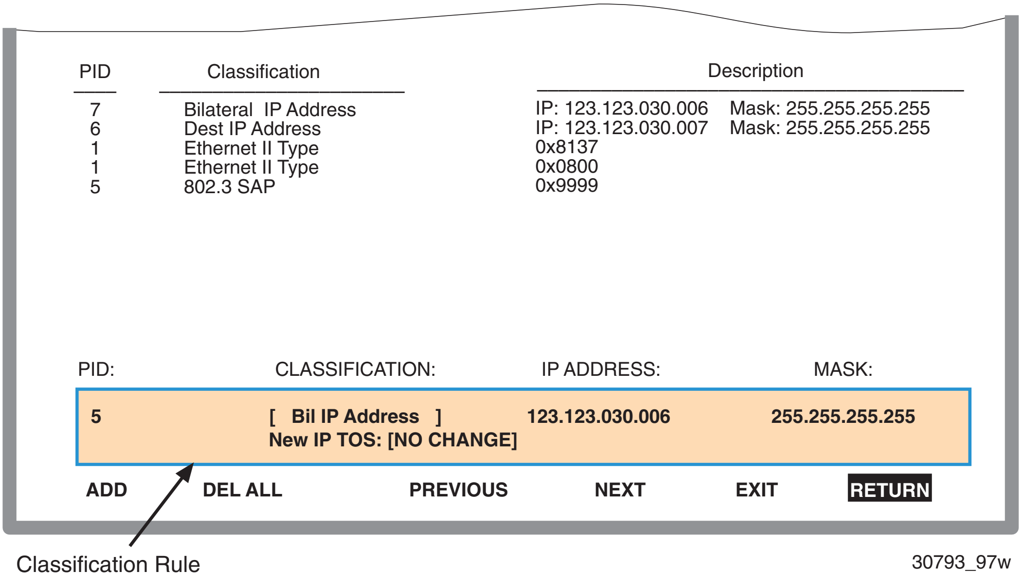
When a frame is received that already contains an 802.1Q frame tag, frame classification is not implemented. Instead, the frame is processed by the SmartSwitch device according to the information contained in the 802.1Q frame tag.

How to Access

Use the arrow keys to highlight the **PRIORITY CLASSIFICATION CONFIGURATION** menu item on the 802.1p Configuration Menu screen and press ENTER. The Priority Classification Configuration screen, Figure 8-6, displays.

Screen Example

Figure 8-6 Priority Classification Configuration Screen



```
PID     Classification          Description

 7      Bilateral  IP Address   IP: 123.123.030.006   Mask: 255.255.255.255
 6      Dest IP Address         IP: 123.123.030.007   Mask: 255.255.255.255
 1      Ethernet II Type        0x8137
 1      Ethernet II Type        0x0800
 5      802.3 SAP               0x9999

PID:            CLASSIFICATION:          IP ADDRESS:          MASK:

5               [  Bil IP Address  ]     123.123.030.006      255.255.255.255
                New IP TOS: [NO CHANGE]
```

Field Descriptions

Refer to Table 8-6 for a functional description of each screen field.

Table 8-6 Priority Classification Configuration Screen Field Descriptions

Use this field …	To…
PID – top of screen (Selectable)	Display the Priority Identifiers (PIDs) currently associated with protocol classifications. To see which ports are assigned to a PID/Classification, or to add/remove a port from a PID/Classification, used in the Protocol Port Configuration screen. For details, refer to Section 8.6.3.
Classification – top of screen (Selectable)	Display the classification associated with the priority in the PID column and may be selected to call up the Protocol Port Configuration screen.
Description (Selectable)	Provide a brief description of the classification.

Table 8-6 Priority Classification Configuration Screen Field Descriptions (Continued)

Use this field …	To…
PID – bottom of screen (Modifiable)	Enter the priority value that will be associated with the classification selected in the Classification field. A PID from 0 to 7 may be typed into the field, where 0 is the lowest priority and 7 is the highest priority. For details on how to enter the PID/Classification, refer to Section 8.6.4.
Classification – bottom of screen (Selectable)	Select the classification that will be associated with the priority selected in the PID field. Depending on the classification selected, there can be up to three fields involved (CLASSIFICATION, IP ADDRESS, and MASK). At the time of this printing, the selections available in each field are listed in Table 8-7. **NOTE:** Besides the PID selected, the order in which a frame is transmitted also depends on the Classification Precedence Rules discussed in Section 8.6.1. These rules come into effect when there are multiple classifications configured in the SmartSwitch device. For details on how to use the Priority Classification Configuration screen to select the classification rule, refer to Section 8.6.4.
ADD (Toggle)	Add the current Classification Rule (PID and Classification selections) to the screen. For details about how to add an entry, refer to Section 8.6.4.
DEL ALL/DEL MARKED (Toggle)	Delete all or one or more marked entries, simultaneously. The DEL ALL command is the default and it is used to simultaneously delete all the configured information Classification Rules. The DEL MARKED command appears in place of the DEL ALL command when one or more lines are marked for deletion. For details on using the two commands, refer to Section 8.6.5.

Table 8-7 provides a list of the Classifications that can be selected in the Classification field and the associated subclassifications.

Table 8-7 Classification List

Classification	Subclassification and Options	Custom or Mask Value
Ethernet II Type>	Ethernet II Type:	
	- IPX	
	- DOD IP	
	- ARP	
	- RARP	
	- AppleTalk	
	- Banyan Vines	
	- DECNET	
	- CUSTOM >	Type Value: 0x**0000**[1]
802.3 SAP>	SSAP/DSAP (802.3):	
New IP TOS:	- IP	
- NO CHANGE		
- TOS=PID		
- CUSTOM>	TOS: Value = 0x00	
	(Range: 0 - 255)	
Same	- IPX	
Same	- IPX RAW	
Same	- BANYAN	
Same	- SNA	
Same	- CUSTOM >	DSAP/SSAP Type: 0x**0000**
For more information about IP TOS, refer to Section 8.6.2.		
IP TOS	Type of Service:	
New IP TOS:	0x**0000**	
- NO CHANGE		
- TOS=PID		
- CUSTOM>	TOS: Value = 0x00	
	(Range: 0 - 255)	

Table 8-7 Classification List (Continued)

Classification	Subclassification and Options	Custom or Mask Value
IP Protocol Type	IP Protocol Type:	
New IP TOS:	TCP	
- NO CHANGE		
- TOS=PID		
- CUSTOM>	TOS: Value = 0x00	
	(Range: 0 - 255)	
Same	- UDP	
Same	- ICMP	
Same	- IGMP	
Same	- OSPF	
Same	- CUSTOM >	Protocol Type: **000**
IPX COS	IPX Class of Service:	
	000	
IPX Packet Type	IPX Packet Type:	
	- Hello or SAP	
	- RIP	
	- Echo Packet	
	- Error Packet	
	- Netware 386/SAP	
	- Seq. Pkt Protocol	
	- Netware 286	
	- CUSTOM >	IPX Packet Type: **00**
Src IP Address	IP Address:	Mask:
New IP TOS:	**000.000.000.000**	**000.000.000.000**
- NO CHANGE		
- TOS=PID		
- CUSTOM>	TOS: Value = 0x00	
	(Range: 0 - 255)	

Table 8-7 Classification List (Continued)

Classification	Subclassification and Options	Custom or Mask Value
Dest IP Address	IP Address:	Mask:
New IP TOS:	**000.000.000.000**	**000.000.000.000**
- NO CHANGE		
- TOS=PID		
- CUSTOM>	TOS: Value = 0x00	
	(Range: 0 - 255)	
Bil IP Address	IP Address:	Mask:
New IP TOS:	**000.000.000.000**	**000.000.000.000**
- NO CHANGE		
- TOS=PID		
- CUSTOM>	TOS: Value = 0x00	
	(Range: 0 - 255)	
Src IPX Network	IPX Network Num:	
	0x**00000000**	
Dest IPX Network	IPX Network Num:	
	0x**00000000**	
Bil IPX Network	IPX Network Num:	
	0x**00000000**	

Table 8-7 Classification List (Continued)

Classification	Subclassification and Options	Custom or Mask Value
Src UDP Port	IP UDP Port:	
New IP TOS:	- FTP Data	
- NO CHANGE		
- TOS=PID		
- CUSTOM>	TOS: Value = 0x00 (Range: 0 - 255)	
Same	- FTP	
Same	- BOOTP Server	
Same	- BOOTP Client	
Same	- RIP	
Same	- Telnet	
Same	- TFTP	
Same	- HTTP	
Same	- DNS	
Same	- SMTP	
Same	- POP3	
Same	- IMAP2	
Same	- IMAP3	
Same	- NETBIOS Name Serv	
Same	- NETBIOS Datagram	
Same	- NETBIOS Sess Serv	
Same	- CUSTOM >	UDP Port Number: **00000**
Dest UDP Port	IP UDP Port:	
Same selections as for Src UDP Port	Same selection as for Src UDP Port Classification	UDP Port Number: **00000**
Bil UDP Port	IP UDP Port:	
Same selections as for Src UDP Port	Same selection as for Src UDP Port Classification	UDP Port Number: **00000**

Table 8-7 Classification List (Continued)

Classification	Subclassification and Options	Custom or Mask Value
Src TCP Port	TCP Port:	
New IP TOS:	- FTP Data	
- NO CHANGE		
- TOS=PID		
- CUSTOM>	TOS: Value = 0x00	
	(Range: 0 - 255)	
Same	- FTP	
Same	- BOOTP Server	
Same	- BOOTP Client	
Same	- RIP	
Same	- Telnet	
Same	- TFTP	
Same	- HTTP	
Same	- DNS	
Same	- SMTP	
Same	- POP3	
Same	- IMAP2	
Same	- IMAP3	
Same	- NETBIOS Name Serv	
Same	- NETBIOS Datagram	
Same	- NETBIOS Sess Serv	
Same	- CUSTOM >	TCP Port Number: **00000**
Dest TCP Port	TCP Port:	
Same selections as for Src TCP Port	Same selection as for Src TCP Port Classification	TCP Port Number: **00000**
Bil TCP Port	TCP Port:	
Same selections as for Src TCP Port	Same selection as for Src TCP Port Classification	TCP Port Number: **00000**

Table 8-7 Classification List (Continued)

Classification	Subclassification and Options	Custom or Mask Value
Src IPX Socket	IPX Socket: - NCP - SAP - RIP - NETBIOS - Diagnostics - NLSP - IPX WAN - CUSTOM >	IPX Socket Type: **00000**
Dest IPX Socket	IPX Socket: Same selection as for Src IPX Socket Classification	IPX Socket Type: **00000**
Bil IPX Socket	IPX Socket: Same selection as for Src IPX Socket Classification	IPX Socket Type: **00000**
Src MAC Address	MAC Address: **00-00-00-00-00-00**	
Dest MAC Address	MAC Address: **00-00-00-00-00-00**	
Bil MAC Address	MAC Address: **00-00-00-00-00-00**	
IP Fragments[2] New IP TOS: - NO CHANGE - TOS=PID - CUSTOM>	TOS: Value = 0x00 (Range: 0 - 255)	

Table 8-7 Classification List (Continued)

Classification	Subclassification and Options	Custom or Mask Value
IP Fragments[2]	Start:	End:
New IP TOS:	00000	00000
- NO CHANGE		
- TOS=PID		
- CUSTOM>	TOS: Value = 0x00	
	(Range: 0 - 255)	
Dest UDP Range	Start:	End:
New IP TOS:	00000	00000
- NO CHANGE		
- TOS=PID		
- CUSTOM>	TOS: Value = 0x00	
	(Range: 0 - 255)	
Bil UDP Range	Start:	End:
New IP TOS:	00000	00000
- NO CHANGE		
- TOS=PID		
- CUSTOM>	TOS: Value = 0x00	
	(Range: 0 - 255)	
Src TCP Port	Start:	End:
New IP TOS:	00000	00000
- NO CHANGE		
- TOS=PID		
- CUSTOM>	TOS: Value = 0x00	
	(Range: 0 - 255)	

Table 8-7 Classification List (Continued)

Classification	Subclassification and Options	Custom or Mask Value
Dest TCP Port	Start:	End:
New IP TOS:	00000	00000
- NO CHANGE		
- TOS=PID		
- CUSTOM>	TOS: Value = 0x00	
	(Range: 0 - 255)	
Bil TCP Port	Start:	End:
New IP TOS:	00000	00000
- NO CHANGE		
- TOS=PID		
- CUSTOM>	TOS: Value = 0x00	
	(Range: 0 - 255)	

1. **Bold** type indicates a user entry.
2. Any fragmented IP frame received is Classified to the priority identification (PID) and forwarded out the ports configured in the Protocol Port Configuration screen.

8.6.1 Classification Precedence Rules

NOTE: It is important that you have a comprehensive understanding of the precedence concept before configuring the SmartSwitch device, as these rules can have a significant impact on the network operation.

When there are multiple classifications assigned to a SmartSwitch device, the SmartSwitch device must determine which classification takes precedence according to the Classification Precedence Rules. The order of precedence is predefined in the SmartSwitch device and cannot be changed.

Table 8-8 lists the ISO Layer, associated classification and precedence levels.

NOTE: In Table 8-8, the following applies:

- Highest precedence is 1a.
- Lowest precedence is 6.
- Exact Match indicates a match of an explicitly defined address.
- Best Match indicates a match of an entire subnet, or range of addresses within a subnet.

Table 8-8 Classification Precedence

Classification Type	Precedence Level
Layer 2	
Source MAC Address Best Match	1a
Destination MAC Address Best Match	1b
EtherType	6
SAP	6
Layer 3	
IP TOS	5a
IP Type	5b
IPX COS	5a
IPX Type	5b
Layer 3	
Source IP Address Exact Match	2a
Source IP Address Best Match	2b
Destination IP Address Exact Match	2c
Destination IP Address Best Match	2d

Table 8-8 Classification Precedence (Continued)

Classification Type	Precedence Level
Layer 3 (Continued)	
Source IPX Network Number	2a
Destination IPX Network Number	2b
IP Fragments	3
Layer 4	
UDP Port Source	4a
UDP Port Destination	4b
TCP Source Port	4a
TCP Destination Port	4b
IPX Socket Source	4a
IPX Socket Destination	4b
UDP Source Port	4a
UDP Source Port Range	4b
UDP Dest Port	4c
UDP Dest Port Range	4d
TCP Source Port	4a
TCP Source Port Range	4b
TCP Dest Port	4c
TCP Dest Port Range	4d

The following example shows how the precedence concept can be applied:

Example

A network administrator has defined the following two classifications involving priorities:

- All frames with an IP TOS value of AA (Layer 3, precedence level 5a) are assigned to priority 7.
- All frames with a TCP source port number of 80 (Layer 4, precedence level 4a) are assigned to priority 3.

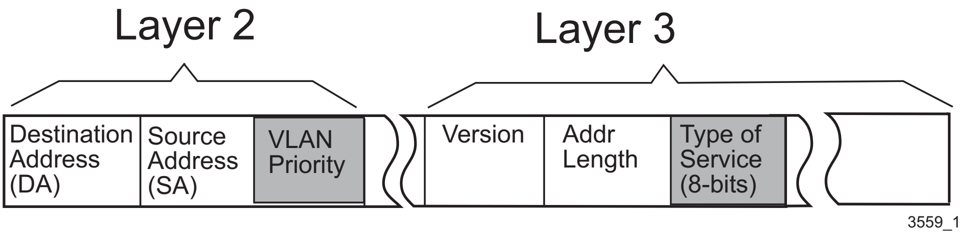
In this example, a frame that is received with a TOS value of AA, and a TCP port number of 80, will be assigned to priority 3. This is because the TCP port number classifications take precedence over IP TOS classifications.

It is important to remember that the SmartSwitch device will classify frames based on one of the classification options.

8.6.2 About the IP TOS Rewrite Function

The Type of Service (TOS) field [also known as the Differential Services (DF) field in RFC 2474] is an 8-bit field. It is located in the IP packet and used by a device to indicate the precedence or priority of a given frame (see Figure 8-7). The TOS layer-3 priority indicator enables the ability to signal the frame priority from end to end as the frame makes its way through the network.

Figure 8-7 Datagram, Layer 2 and Layer 3



This IP TOS Rewrite feature enables a Network Administrator to assign Layer 3 TOS characteristics to incoming frames and setting the switch to rewrite the 8-bit TOS value in the Layer 3 information portion of incoming frames.

The IP TOS Rewrite feature enables you to configure the switch to:

- Insert a user-defined 8-bit value into the layer-3 TOS field.
- Write over an existing TOS value. This is useful when the Network Administrator wants to enforce a specific priority policy in the network.

The IP TOS Rewrite parameters are set using the Priority Classification screen. The screen enables you to configure the new IP TOS field for any IP frame classification. A selection field is displayed for all supported classification rules. The default value is "NO CHANGE". You can optionally specify TOS=PID, whereby the precedence sub-field in the TOS field to match the value of the priority in the classification rule. You can also specify a CUSTOM TOS value between 0 and 255. This allows you to specify an IP TOS value for a particular need.

8.6.3 Displaying the Current PID/Classification Assignments

To see which ports are set to a particular PID/Classification (Classification Rule), the Protocol Port Configuration screen must be displayed.

To access the Protocol Port Configuration, proceed as follows:

1. Use the arrow keys to step to the **line** with the Classification Rule of interest.
2. Press ENTER. The Protocol Port Configuration screen displays, showing a list of the current ports and those associated with the Classification Rule selected in step 1. These ports are identified on the screen by a **YES** setting. For more information about the Protocol Port Configuration screen and how to use it, refer to Section 8.7.

8.6.4 Assigning a Classification to a PID

NOTE: It is strongly recommended that you read Section 8.6.1 for more information concerning classification before configuring the SmartSwitch device. Incorrect configuration will affect network operation.

To add a Classification Rule, proceed as follows:

1. Use the arrow keys to highlight the **PID** (priority identification) field.
2. Type in the appropriate priority (**0** through **7**), where 0 is the lowest priority and 7 is the highest priority. Press ENTER.
3. Use the arrow keys to highlight the **Classification** field.
4. Press the SPACE bar to step to the appropriate Classification. Table 8-7 lists the subclassification associated with each Classification (examples of classifications: Ethernet II Type, 802.3 SAP, IP TOS, IP Protocol Type, etc.).
5. Use the arrow keys to highlight the subclassification field to the immediate right of the Classification field. The name of the field changes depending on the selected Classification, as shown in Table 8-7 (examples of subclassification: Ethernet II Type, SSAP/DSAP (802.3), Type of Service, IP Protocol Type, etc.).

6. Press the SPACE bar to step to the appropriate protocol. In some cases, there is only one selection and a value needs to be entered. This is indicated by **bold** zeros. Table 8-7 lists the possible selections associated with each subclassification (examples: IPX, AppleTalk, NetBIOS, Banyan Vines, **000.000.000.000**, 0x**00000000**, etc.).
7. In some cases, a selection in the subclassification field requires a value to be entered in a third field to the right of the subclassification field. If so, use the arrow keys to highlight that third field and type in the appropriate value. Otherwise, go to step 8.
8. Use the arrow keys to highlight the **ADD** command field.
9. Press ENTER to save the PID and Classification settings. After a brief delay, the Classification Rule (PID, Classification, and Description) displays in the top half of the screen.

NOTE: After creating a classification rule you must assign it to the appropriate ports using the Protocol Port Configuration screen described in Section 8.7.

8.6.5 Deleting PID/Classification/Description Line Items

All, or one or more, line items can be deleted as follows:

Deleting All Line Items

To delete all configured Classification Rules, use the arrow keys to highlight the **DEL ALL** command field and press ENTER.

Deleting One or More Line Items

To delete one or more Classification Rules, mark each entry and then delete them, as follows:

1. Use the arrow keys to highlight a **line** to be deleted.
2. Press the M key and an asterisk (*) appears next to the highlighted line to mark it. The DEL ALL command is changed to DEL MARKED.
3. If more than one line item is to be deleted, repeat steps 1 and 2 to mark each line.

NOTE: To remove a mark, perform steps 1 and 2. Pressing M when a marked line is highlighted will remove the mark. If all marks are removed, the DEL MARKED command is changed back to DEL ALL.

4. After the lines are marked, use the arrow keys to highlight the **DEL MARKED** command field.
5. Press ENTER. The marked line items are deleted and the DEL MARKED command is changed back to DEL ALL.

8.7 PROTOCOL PORT CONFIGURATION SCREEN

When to Use

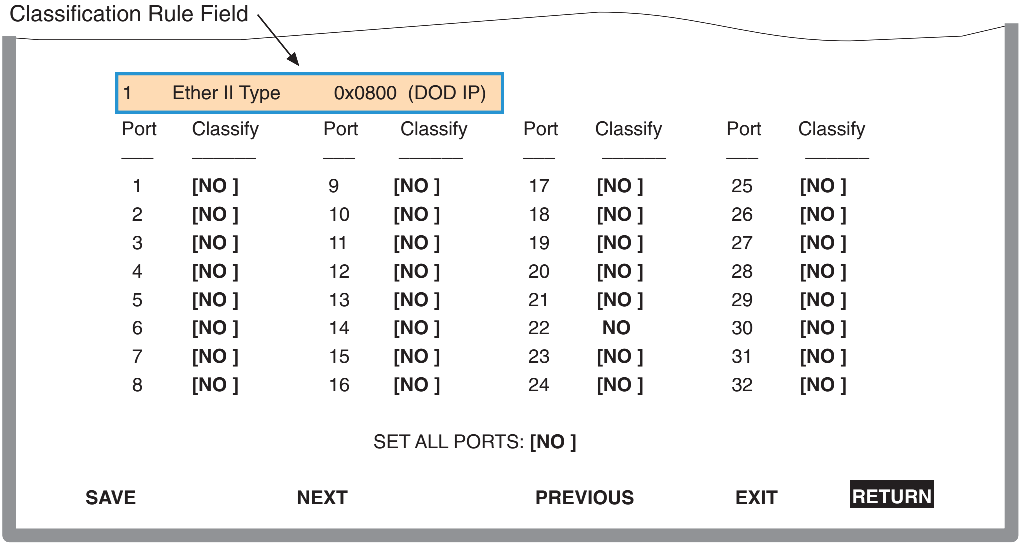
To display the ports associated with the line item (Classification Rule) selected in the Priority Classification Configuration screen described in Section 8.6. Each port can be changed so it will or will not transmit frames according to the Classification Rule.

How to Access

Use the arrow keys to highlight the line of interest (Classification Rule) under the Priority/Protocol Type/Configured Ports columns on the Priority Classification Configuration screen and press ENTER. The Protocol Port Configuration screen, Figure 8-8, displays. The Classification Rule used to access this screen is displayed in the Classification Rule field shown in Figure 8-8.

Screen Example

Figure 8-8 Protocol Port Configuration Screen



Classification Rule Field

```
1      Ether II Type        0x0800  (DOD IP)

Port   Classify       Port   Classify      Port   Classify      Port   Classify
____   ______         ____   ______        ____   ______        ____   ______

  1    [NO ]            9    [NO ]          17    [NO ]          25    [NO ]
  2    [NO ]           10    [NO ]          18    [NO ]          26    [NO ]
  3    [NO ]           11    [NO ]          19    [NO ]          27    [NO ]
  4    [NO ]           12    [NO ]          20    [NO ]          28    [NO ]
  5    [NO ]           13    [NO ]          21    [NO ]          29    [NO ]
  6    [NO ]           14    [NO ]          22     NO            30    [NO ]
  7    [NO ]           15    [NO ]          23    [NO ]          31    [NO ]
  8    [NO ]           16    [NO ]          24    [NO ]          32    [NO ]

                         SET ALL PORTS: [NO ]

SAVE           NEXT              PREVIOUS           EXIT         RETURN
```

30691_47

Field Descriptions

Refer to Table 8-9 for a functional description of each screen field.

Table 8-9 Protocol Port Configuration Screen Field Descriptions

Use this field…	To…
Classification Rule (Read-Only)	See the Classification Rule (Priority, Classification, and Definition) of the line selected in the Priority Classification Configuration screen. For example, in Figure 8-8, the Classification Rule – 1, Ether II Type, 0x0800 (DOD IP) – was selected in the Priority Classification Configuration screen to access the Protocol Port Configuration screen. All ports with YES in the Classify columns would be those ports associated with PID 1 with an Ether II Type Classification. This causes Ether II Type frames received by those ports to be transmitted with a priority value of 1 and according to the Classification Precedence Rules.
Port (Read-Only)	See the number of each port.
Classify (Toggle)	See which ports are set to the PID/Classification indicated in the Classification Rule field (see Figure 8-8). The Classify field toggles between YES and NO, which determines whether or not the associated port is set to the Classification Rule. **NOTE:** As each Classify field is highlighted, the Event Message Line (not shown) at the top of the screen indicates the port type. For example: Fast Ethernet Front Panel, FTM Backplane Port 3, and Gigabit Ethernet VHSIM. If a port cannot be configured, “NO” displays without brackets. For details about assigning ports, refer to Section 8.7.1.
SET ALL PORTS (Toggle)	Toggle between YES and NO. This determines whether or not all ports will be assigned to the classification rule shown in the Classification Rule field. NO is the default. For details about setting all ports simultaneously, refer to Section 8.7.1.

8.7.1 Assigning Ports to a PID/Classification

To assign one or more ports, or all ports simultaneously, to a PID/Classification (Classification Rule), proceed as follows:

Assigning One or More Ports Individually

1. Use the arrow keys to highlight the **Classify** field adjacent to the Port number.
2. Press the SPACE bar to toggle the Classify field to either **NO** or **YES**. YES associates the port to the priority shown in the Classification Rule field.
3. If more than one port is being set, repeat the first two steps for each port.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
5. Press ENTER. The message “SAVED OK” displays and the settings are saved.

Assigning All Ports Simultaneously

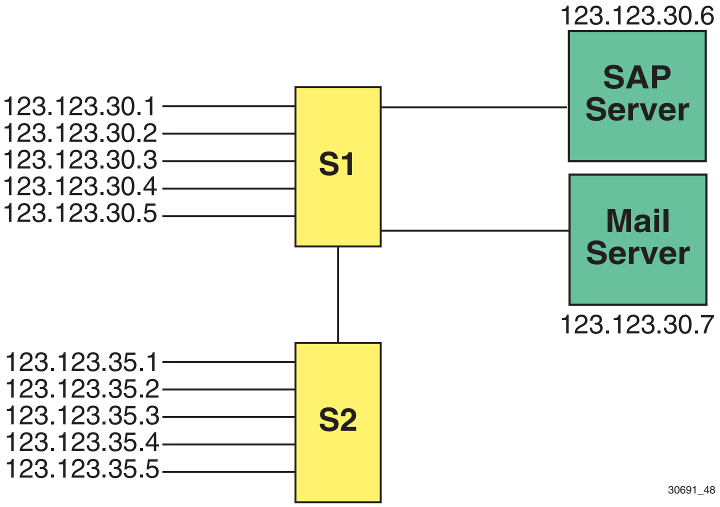
1. Use the arrow keys to highlight the **SET ALL PORTS** command field.
2. Press the SPACE bar to toggle the SET ALL PORTS field to **YES** or **NO** and press ENTER. This setting determines whether or not all the ports are set to the PID/Classification shown in the Classification Rule field.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays and the setting is saved.

Example

This example illustrates how to prioritize network traffic using classification rules.

In this example, illustrated in Figure 8-9, the ABC Company wants to prioritize traffic to their SAP server and Mail server, so that the SAP Server has the highest priority, and the Mail Server, the lowest priority.

Figure 8-9 Prioritizing Network Traffic According to Classification Rule



8.7.2 Solving the Problem

In this example, switches S1 and S2 have already been configured and are operating. The following covers only the additional steps needed to configure each switch to establish the priority for each server.

NOTE: For optimal operation of the prioritizing function, the connection between S1 and S2 is set for 802.1Q tagging.

Switch 1

The following settings are done using the Priority Classification Configuration screen to assign the classification to the priority. Then the Protocol Port Configuration screen is used to assign the ports to the appropriate priority and classification.

NOTE: In the two settings below, the subnet mask is set to 255.255.255.255. This means that frames with a source or destination address of 123.123.30.6 or 123.123.30.7 will be mapped as a priority 7 or 0, respectively.

1. To set the SAP Server (IP 123.123.30.6) to the highest priority (7), the following settings will be made using the Priority Classification Configuration screen:
   - PID: 7
   - Classification: Bil IP Address
   - IP Address: 123.123.30.6
   - Data Mask: 255.255.255.255
2. Assign all ports on the SmartSwitch device to use this classification setting.
3. To set the Mail Server (IP 123.123.30.7) to the lowest priority (0), the following settings will be made using the Priority Classification Configuration screen:
   - PID: 0
   - Classification: Bil IP Address
   - IP Address: 123.123.30.7
   - Data Mask: 255.255.255.255
4. Assign all ports on the SmartSwitch device to use this classification setting.

Switch 2

The Switch 1 setup instructions are repeated to set up Switch 2.

NOTE: For optimal operation of the prioritizing function, the connection between S1 and S2 is set for 802.1Q tagging.

8.8 RATE LIMITING CONFIGURATION SCREEN

NOTE: The Inbound Rate Limiting function is not supported on ports connected to SmartTrunk segments.

When to Use

To limit the rate of traffic entering and leaving the SmartSwitch device on a per port/priority basis. Up to three inbound rules and three outbound rules can be programmed per port to control traffic according to the priority entries. The rules also contain the programmed traffic rate. The allowable range for the rate limit is 1 Kbps to 1 Gbps.

The outbound and inbound rate limit is configured for a given port and list of priorities. The list of priorities can include one, some, or all of the eight 802.1p priority levels. The combined rate of all traffic entering and exiting the port with the priorities configured to that port is not allowed to exceed the programmed limit. If the rate exceeds the programmed limit, frames are dropped until the rate falls below the limit.

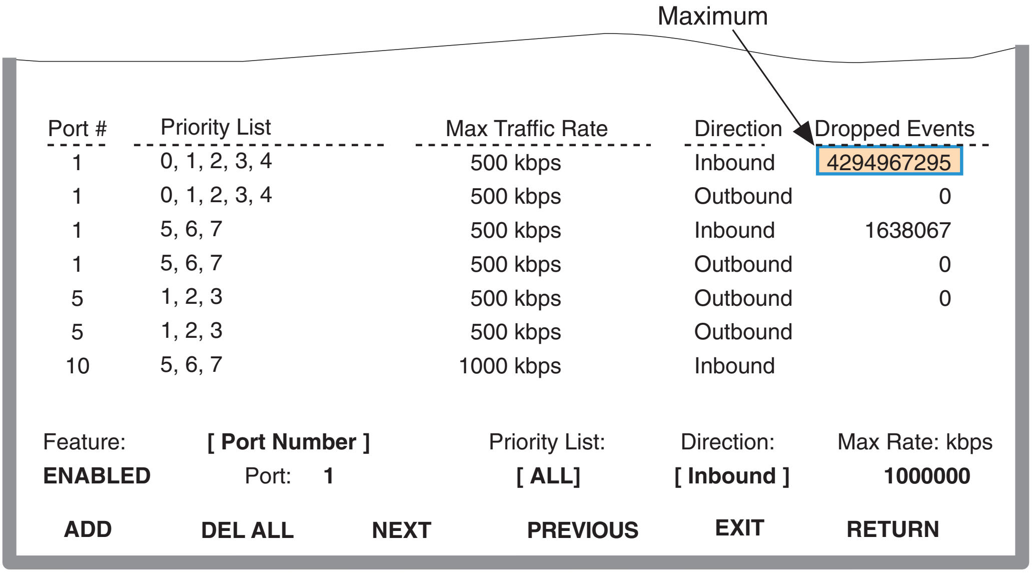
For more information about the application of Rate Limiting and an example of how it can be used, refer to Section 8.8.3.

How to Access

Use the arrow keys to highlight the **RATE LIMITING** menu item on the 802.1p Configuration Menu screen and press ENTER. The Rate Limiting Configuration screen, Figure 8-10, displays.

Screen Example

Figure 8-10 Rate Limiting Configuration Screen



```
Port #   Priority List          Max Traffic Rate    Direction   Dropped Events
------   ---------------------  ------------------  ---------   --------------
   1     0, 1, 2, 3, 4              500 kbps         Inbound      4294967295
   1     0, 1, 2, 3, 4              500 kbps         Outbound              0
   1     5, 6, 7                    500 kbps         Inbound         1638067
   1     5, 6, 7                    500 kbps         Outbound              0
   5     1, 2, 3                    500 kbps         Outbound              0
   5     1, 2, 3                    500 kbps         Outbound
  10     5, 6, 7                   1000 kbps         Inbound

Feature:        [ Port Number ]        Priority List:   Direction:    Max Rate: kbps
ENABLED           Port:    1             [ ALL]        [ Inbound ]      1000000

  ADD        DEL ALL      NEXT      PREVIOUS      EXIT       RETURN
```

Field Descriptions

Refer to Table 8-10 for a functional description of each screen field.

Table 8-10 Rate Limiting Configuration Screen Field Descriptions

Use this field…	To…
Port # (Read-Only)	See the number of each configured port. The same port number may appear four times, but with different priorities assigned. **NOTE:** If the configuration for a port needs to be changed, delete the line containing the incorrect configuration, and then enter a new configuration with the correct settings.
Priority List – top of screen (Read-Only)	See the priorities associated with each port entry.

Table 8-10 Rate Limiting Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Max Traffic Rate (Read-Only)	See the maximum traffic rate set for each port entry. There can be up to four entries (two for Inbound and two for Outbound traffic) for the same port. However, there must be a different priority for each Inbound entry on a port, and the same holds true for two Outbound entries.
Direction – top of screen (Read-Only)	Show if the port is configured to limit traffic Inbound or Outbound.
Dropped Events (Read-Only)	See the number of frames dropped on each port. Up to 4,294,967,295 dropped frames may be displayed. When the maximum count is reached, the count will roll over to zero. (This screen does not refresh automatically, so you must re-enter the screen to refresh it.)
Feature (Toggle)	Enable or disable the Rate Limiting feature on all configured ports. This field displays the current feature status (ENABLED or DISABLED) and can be toggled between ENABLED and DISABLED. When ENABLED is highlighted, pressing ENTER disables the screen function and the field changes to DISABLED. DISABLED is the default value. **NOTE:** This field **must** be enabled for the Rate Limiting feature to function.
Port Number (Modifiable) or **Port Type** (Selectable)	Enter the number of the port to be configured using the Port Number field, or use the Port Type field to select all the 10 Mbps Ethernet, all the 100 Mbps Ethernet or all the 1 Gbps Ethernet type ports for configuration. The **Port Number** field may be highlighted and toggled to **Port Type** using the SPACE bar. When the Port Number field is displayed (default value), the Port field below it may be highlighted and a port number typed in that field. When Port Type is displayed, the field below may be highlighted and a port type: [all 10Mbps enet], [all 100Mbps enet] or [all Gbps enet] may be selected using the SPACE bar. For details on configuring a port, refer to Section 8.8.1.

Table 8-10 Rate Limiting Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Priority List – bottom of screen (Selectable)	Assign one or more priorities to the port being configured. The settings available are 0, 1, 2, 3, 4, 5, 6, 7, or ALL. When the Priority List is highlighted, the SPACE bar is used to step to the priority, which must be marked with an asterisk (*) using the M key. More than one priority may be selected and marked for each port. **NOTE:** If there are two entries for Inbound traffic with the same Port number (for example, Port 2 and Port 2), you cannot assign the same priority to both Port Inbound entries. This also holds true for two entries for Outbound traffic on the same port. The selected priorities can be cleared by stepping to each one and pressing the M key. For details on configuring a port, refer to Section 8.8.1.
Direction – bottom of screen (Toggle)	Toggle between Inbound and Outbound rate limiting. Inbound is the default value. Up to four rate limit rules (entries) may be set per port, two for Inbound and two for Outbound or any combination of the four Inbound or Outbound. Inbound refers to traffic being received by the SmartSwitch device and Outbound refers to traffic leaving the SmartSwitch device. Inbound configures the rate limit to drop frames when the traffic rate (Kbps) received by the switch port exceeds the setting in the Max Rate: Kbps field for a particular entry. If there are two or three priority port entries set to Inbound, each entry functions independently. So, if the Max Rate is exceeded in one entry, the frames in that entry are dropped. However, if the traffic associated with another other entry on the same port is transmitting within its maximum rate setting, the frames on that port are not affected. Outbound functions the same as the Inbound, except that the port is configured to drop frames when the traffic rate (Kbps) out of the port exceeds the setting in the Max Rate: Kbps field for a particular entry.

Table 8-10 Rate Limiting Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Max Rate: kbps (Modifiable)	Enter the maximum transmission rate for this entry. The maximum transmission rate includes all frames associated with the priorities selected in the Priority List field. The default is the high setting of 100 Kbps maximum interface speed. The high range setting is 100 Kpbs to 1 Gbps. The low range setting is 50 to 40000 Kpbs. For details on rate limiting, refer to Section 8.8.1. **NOTE:** For further details on configuring the rate limiting range on a port, refer to the rate_limit_mode command in Section 11.2.
ADD (Command)	Add the current port, priority, and maximum rate selections to the screen. For details about how to configure and add an entry, refer to Section 8.8.1.
DEL ALL/DEL MARKED (Toggle)	Delete all or one or more marked entries. The DEL ALL command is the default and it is used to simultaneously delete all the lines of configured information. The DEL MARKED command appears in place of the DEL ALL command when one or more lines are marked for deletion. For details on using the two commands, refer to Section 8.8.2.

8.8.1 Configuring a Port

The following describes how to configure a port using the Rate Limiting Configuration screen:

1. To enter a Port Type, proceed to step 2. To enter a port number, proceed as follows:

   a. Use the arrow keys to highlight the field (**1**) below the **Port Number** field.

   b. Type in the port number and press ENTER.

   c. Proceed to step 3.

2. To enter a Port Type, proceed as follows:

   a. Use the arrow keys to highlight the **Port** field (near the bottom of the screen) and press the SPACE bar. **Port Number** changes to **Port Type** and the field below it changes to **[all 10Mbps enet]**.

   b. Use the arrow keys to highlight the **[all 10Mbps enet]** field below the Port Type field.

   c. If the port type **[all 10Mbps enet]** is not the selection needed, press the SPACE bar to select either **[all 100Mbps enet]** or **[all 1Gbps enet]**.

3. Use the arrow keys to highlight the field below the **Priority List** field, near the bottom of the screen.

4. Select the priority setting(s) for the port as follows:

   a. Use the SPACE bar to step to a priority setting: **ALL**, **0**, **1**, **2**, **3**, **4**, **5**, **6**, or **7**.

   b. Press the **M** key to mark the desired priority with an asterisk.

   c. If more than one priority is to be selected for the port being configured, repeat steps a and b for each additional selection.

NOTE: At least one priority must be marked to create an entry.

5. Use the arrow keys to highlight the **Direction** field, near the bottom of the screen.

6. Use the SPACE bar to toggle to either **Inbound** or **Outbound**.

7. Use the arrow keys to highlight the field below the **Max Rate: kbps** field.

8. Type in the maximum rate in Kbps (minimum: 50 Kbps, maximum is dependent on the speed capability of the port). For further information, refer to the rate_limit_ command in Chapter 11.

9. To add the new port configuration to memory, highlight the **ADD** command field and press ENTER. The new entry displays in the screen.

10. Repeat steps 1 through 9 of this procedure to configure additional ports Inbound or Outbound limits on the same port.

11. If Inbound or Outbound rate limiting entries are to be configured on other ports on the device, repeat steps 1 through 10 to configure each port. Any combination of Inbound and Outbound entries may be configured per port with a limit of three for Inbound and three for Outbound. (For example, two inbound/two outbound, one inbound/two outbound, two inbound/one outbound and one inbound/one outbound.)

12. After configuring the entry(ies) on the ports, enable the screen function for all the configured ports by highlighting DISABLED in the Feature field and pressing ENTER. The screen function is enabled and the Feature field changes to ENABLED.

8.8.2 Changing/Deleting Port Line Items

All, or one or more, line items containing the configured port and its priority, maximum rate, and associated dropped frames can be changed/replaced or deleted as follows:

Changing One or More Line Items

To change the configuration values in a line item, that line item must be deleted and replaced with a new entry with the correct configuration values. The new settings can then be configured and added.

Deleting All Line Items

To delete all configured line items, use the arrow keys to highlight the **DEL ALL** command field and press ENTER.

Deleting One or More Line Items

To delete one or more line items, mark each entry and then delete them, as follows:

1. Use the arrow keys to highlight a **line** to be deleted.
2. Press the M key and an asterisk (*) appears next to the highlighted line to mark it. The DEL ALL command is changed to DEL MARKED.
3. If more than one line item is to be deleted, repeat steps 1 and 2 to mark each line.

NOTE: To remove a mark, perform steps 1 and 2. When a marked line is highlighted, pressing M will remove the mark. If all marks are removed, the DEL MARKED command is changed back to DEL ALL.

4. After the lines are marked, use the arrow keys to highlight the **DEL MARKED** command field.
5. Press ENTER. The marked line items are deleted and the DEL MARKED command is changed back to DEL ALL.

8.8.3 More About Rate Limiting

Rate Limiting enables Service Providers in Multi-Dwelling-Unit (MDU) and similar environments to offer varied bandwidth to customers using low cost Ethernet connections. Another solution for the enterprise, is to provide high priority bandwidth on the network for guaranteed service level agreements.

NOTE: When allocating the maximum rate per port, the maximum bandwidth of the uplink must be kept in mind. For example, if the ports are all set to 10 Mbps and there are 24 ports, this equals 240 Mbps of bandwidth. If the uplink is only 100 Mbps, there is an obvious problem if the network administrator guaranteed more bandwidth than the uplink can support.

In Multi-Dwelling Unit (MDU) or similar environments, the Rate Limiting feature can be activated per port to adjust the usable bandwidth on a 10 Mbps Ethernet or other type of physical connection. In residential housing, the service provider may offer multiple internet service packages, each offering different bandwidth at a different price. These offerings can be supported using low cost 10 Mbps Ethernet ports wired to each dwelling.

In the enterprise network, this feature (combined with Layer 3/4 prioritization) can provide guaranteed delivery of high priority traffic through a congested network fabric. This is accomplished through the construction of a committed information rate (CIR) fabric within the traditional best effort enterprise LAN fabric.

Example

This is a simple example intended to show how the Rate Limiting feature can be applied to solve a problem.

Assume that a network was built using SmartSwitch 6000 chassis in each wiring closet and interconnected with SmartSwitch Routers using Gigabit Ethernet links. Also, assume that 100 users are attached to each SmartSwitch 6000 chassis through 100 Mbps Ethernet ports. If each user attempted to transfer data out of the wiring closet at the maximum possible rate, there could be up to 10 Gbps (100 users x 100 Mbps) of traffic attempting to leave the chassis over a single gigabit link. In this situation, much of the traffic will be arbitrarily dropped.

Now assume that the system administrator wants to guarantee the delivery of SAP R/3 traffic by prioritizing it above all other incoming traffic to the chassis. (Unless the inbound rate of the SAP traffic can be controlled, the guarantee still cannot be made because of the potential for oversubscription of the inbound gigabit link by high priority traffic.)

To solve this problem, the Rate Limiting feature can be configured on each port to provide each user with 5 Mbps of high priority bandwidth into the fabric. Now the maximum possible amount of traffic attempting to leave the chassis at high priority is 5 x 100 = 500 Mbps. The gigabit link has ample capacity to carry this load out of the chassis. Similar provisioning calculations must be carried throughout the network all the way to the particular resources to which the service guarantee applies. The sum of the rate limits on all user ports cannot exceed the capacity of the weakest point in the delivery path to the resource.

9

Layer 3 Extensions Menu Screens

This chapter describes the Layer 3 Extensions Menu screen and the IGMP/VLAN Configuration screen (Section 9.2).

Screen Navigation Path

Password > Device Menu > Device Configuration Menu > **Layer 3 Extensions Menu**

9.1 LAYER 3 EXTENSIONS MENU SCREEN

When to Use

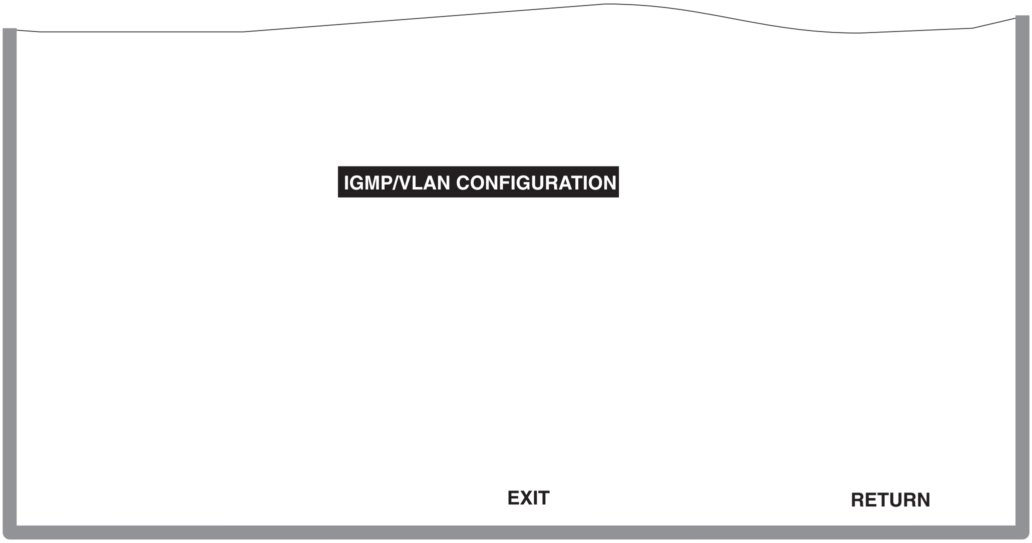
To access the IGMP/VLAN Configuration screen.

How to Access

Use the arrow keys to highlight the **LAYER 3 EXTENSIONS MENU** item on the Device Configuration Menu screen and press ENTER. The Layer 3 Extensions Menu screen, Figure 9-1, displays.

Screen Example

Figure 9-1 Layer 3 Extensions Menu Screen



30691_50

Menu Descriptions

Refer to Table 9-1 for a functional description of each menu item (at this time there is only one menu item).

Table 9-1 Layer 3 Extensions Menu Screen Menu Item Descriptions

Menu Item	Screen Function
IGMP/VLAN CONFIGURATION	Used to enable or disable IGMP (Internet Group Management Protocol) on selected VLANs. For details, refer to Section 9.2.

9.2 IGMP/VLAN CONFIGURATION SCREEN

When to Use

The IGMP/VLAN Configuration screen, Figure 9-2, is used to enable or disable IGMP (Internet Group Management Protocol, RFC 2236) on selected VLANs, or globally on all VLANs that are available.

IGMP Snooping provides a solution for handling multicast streams in layer 3 routers. IGMP is for hosts on multi-access networks to inform locally attached switches of their Multicast group membership information. This is performed by hosts multicasting IGMP Host Membership Reports. Multicast switches listen for these messages and then pass them to other switches. This allows distribution trees to be formed to deliver multicast datagrams.

Information from the IGMP packets is used to send the multicast stream only to the end stations that request it.

IGMP is enabled or disabled by VLAN, not port by port.

NOTE: Certain versions of firmware will not allow the switch to be a querier. Please check your release notes for further information. Refer to RFC 2236, Section 8, for more information on IGMP.

The following multicast routing protocols are transparently supported and are used only to detect the location of routers (See the Release Notes for any changes or additions to this list):

- DVMRP (Distance Vector Multicast Routing Protocol, RFC 1075)
- PIM (Protocol Independent Multicast) version 1 and 2
- CBT (Core Based Trees)
- MOSPF (Multicast OSPF, RFC 1583)

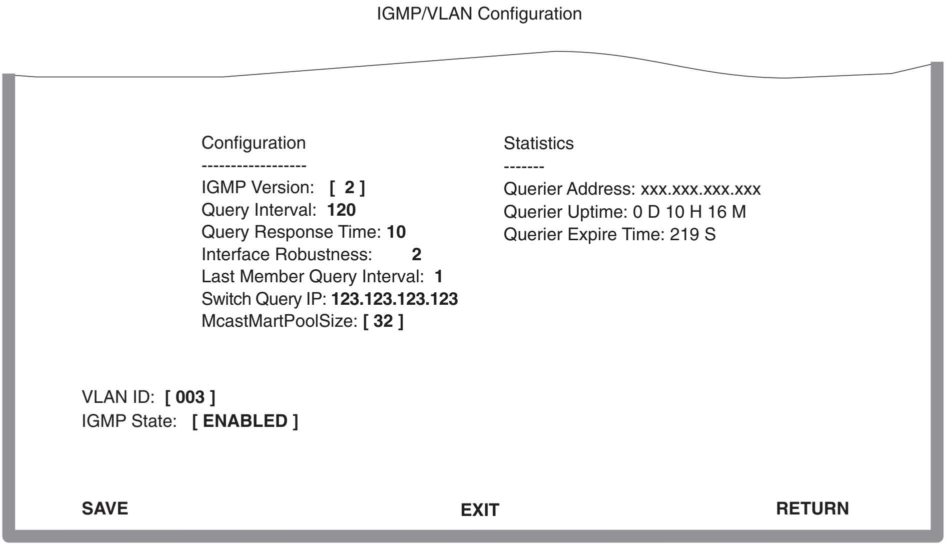
For additional information about IGMP, refer to Appendix B.

How to Access

Use the arrow keys to highlight the **IGMP/VLAN CONFIGURATION** menu item on the Layer 3 Extensions Menu and press ENTER. The IGMP/VLAN Configuration screen, Figure 9-2, displays.

Screen Example

Figure 9-2 IGMP/VLAN Configuration Screen



```
                         IGMP/VLAN Configuration

                  Configuration                      Statistics
                  ------------------                 -------
                  IGMP Version:   [ 2 ]              Querier Address: xxx.xxx.xxx.xxx
                  Query Interval:  120               Querier Uptime: 0 D 10 H 16 M
                  Query Response Time: 10            Querier Expire Time: 219 S
                  Interface Robustness:       2
                  Last Member Query Interval:  1
                  Switch Query IP: 123.123.123.123
                  McastMartPoolSize: [ 32 ]

        VLAN ID:  [ 003 ]
        IGMP State:   [ ENABLED ]

        SAVE                        EXIT                        RETURN
```

25042-105w

Field Descriptions

Table 9-2 describes each field of the IGMP/VLAN Configuration screen.

Table 9-2 IGMP/VLAN Configuration Screen Field Descriptions

Use this field…	To…
IGMP Version (Toggle)	See the current configured IGMP version running on the VLAN selected in the VLAN ID field (version 1 or 2). The default is version 2. The IGMP Version field can be toggled to configure the switch in either version 1 or 2 to match the router configuration. For IGMP to function correctly, all switches on a LAN must be configured to run the same version of IGMP. All VLANs available to the switch will be affected if **ALL** is chosen as the option under VLAN ID. The field will initially display an asterisk (*).

Table 9-2 IGMP/VLAN Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Query Interval (Modifiable)	See or change the query interval time. If the switch is the querier, the value in the Query Interval field indicates how often IGMP Host-Query frames are transmitted on the VLAN selected in the VLAN ID field. This value is also used in calculations for other timers. The default value is 125 seconds. The range of possible entries is 1 to 300 seconds. An entry outside of the range will cause the error message “PERMISSIBLE RANGE: 1...300” to display in the Event Message field. The field will initially display an asterisk (*).
Query Response Time (Modifiable)	Enter the maximum query response time advertised in IGMPv2 general queries on this VLAN. This value is used in calculations for other timers. The default value is 10 seconds. The range of possible entries is 1 to 300 seconds. The value entered in this field cannot be bigger than the Query Interval. The field will initially display an asterisk (*).
Interface Robustness (Modifiable)	Tune the expected frame loss on a subnet. If a subnet is expected to be high loss, the Robustness Variable may be increased. IGMP is robust to (Robustness Variable-1) packet losses. This value is also used in calculations for other timers. The default value is 2. The field will initially display an asterisk (*). **TIP:** If the Interface Robustness is adjusted higher than the default value, depending on the network, this may be an indication of problems with the network that need to be resolved.
Last Member Query Interval (Modifiable)	Modify the leave latency of the network.The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. The interval is in tenths of seconds. This value is not used if the switch is not the querier. The field will initially display an asterisk (*).

Table 9-2 IGMP/VLAN Configuration Screen Field Descriptions (Continued)

Use this field…	To…
Switch Query IP (Modifiable)	Enter the IP address that the switch will use to source IGMP query frames when the switch is the designated querier on the VLAN. The IP address *must* be a valid address associated with the VLAN. The field will initially display an asterisk (*). **NOTE:** To prevent the switch from participating in the IGMP querier election, this IP address *must* be set to 000.000.000.000.
McastMartPoolSize (Selectable)	Select the multicast pool size — the total number of multicast streams supported — using the SPACE bar. Valid values are 16 to 512 in increments of 16. Default is 32. **NOTE:** Modifying the multicast pool size will require a reset of the device.
Querier Address (Read-Only)	See the address of the IGMP Querier on the IP subnet to which this VLAN is attached. The field will initially display an asterisk (*).
Querier Uptime (Read-Only)	See the number of seconds that the current IGMP Querier has been operational since the last change in Queriers. The field will initially display an asterisk (*).
Querier Expire Time (Read-Only)	See the number of seconds remaining before the Other Querier Present Timer expires. If the local system (current device displayed) is the querier, the value of this object is zero. The field will initially display an asterisk (*).

Table 9-2 IGMP/VLAN Configuration Screen Field Descriptions (Continued)

Use this field…	To…
VLAN ID (Modifiable)	Enter the Identifying number of the VLAN to be modified. If there are no VLANs configured for IGMP, NONE is displayed in this field and asterisks (*) will display in the Configuration, Statistics, and IGMP State fields. The information under Configuration and Statistics applies only to this VLAN ID. Use the SPACE bar to step through all available VLAN IDs. The fields that are selectable or modifiable will initially display asterisks (*), then the SPACE bar can be used to display the selectable fields, and the numeric keys can be used to change the modifiable fields. To update the Configuration and Statistics fields for a selected VLAN ID, use the SAVE command.
IGMP State (Selectable)	See the current state of the VLAN indicated in the VLAN ID field, which can be modified. Use the SPACE bar to step through the choices: ENABLED, DISABLED, and DELETE. The commands will act only on the VLAN whose ID is in the VLAN ID field.

9.2.1 IGMP/VLAN Configuration Procedure

To set up IGMP protocol for VLANs, proceed as follows:

1. Use the arrow keys to highlight the **VLAN ID** field, and use the SPACE bar to step through the VLAN choices to find the correct VLAN to configure.

NOTE: The VLAN IDs are those of the VLANs created using the Static VLAN Configuration screen described in Chapter 8.

However, a VLAN ID of a VLAN not yet created can be entered, and the parameters can be configured and saved using the SAVE command. However, the VLAN and its configuration is not functional until that VLAN is created using the Static VLAN Configuration screen. Parameters not modified default according to the MIB.

2. Use the arrow keys to highlight the **IGMP State** field.

3. Use the SPACE bar to select **ENABLED**, **DISABLED**, or **DELETE**. If a specific VLAN was chosen in Step 1, ENABLED and DISABLED are used to enable or disable the IGMP

configuration of the chosen VLAN. (DELETE will remove the IGMP configuration of the VLAN.)

4. Use the arrow keys to highlight the **IGMP Version** field. Then use the SPACE bar to select the proper IGMP version for the VLAN shown in the VLAN ID field.

NOTE: When configuring IGMP, it is advisable to follow the IGMP configuration rules in RFC 2236 concerning switches, and routers.

5. Use the arrow keys to highlight the remaining fields: **Query Interval**, **Query Response Time**, **Interface Robustness**, **Last Member Query Interval**, **Switch Query IP**, and **McastMartPoolSize.** Enter the desired numbers in each field.

6. Use the arrow keys to highlight the **SAVE** command and press the ENTER key to save the information in all the fields that were changed. Repeat this procedure for each VLAN that you want to configure for IGMP.

10

Device Statistics Menu Screens

This chapter describes how to use the Device Statistics Menu screen and the following screens that may be selected from its menu:

- Switch Statistics screen (Section 10.2)
- Interface Statistics screen (Section 10.3)
- RMON Statistics screen (Section 10.4)
- An HSIM or VHSIM Statistics screen may be selected from the Device Statistics Menu screen when an optional HSIM or VHSIM is installed in the SmartSwitch device. For a description of the screen and how to use it, refer to the user's guide for that HSIM or VHSIM.

Screen Navigation Path

Password > Device Menu > **Device Statistics Menu**

10.1 DEVICE STATISTICS MENU SCREEN

When to Use

To obtain the following information:

- Statistics concerning frame traffic through each switch port.
- MIB II statistics for each switched interface.
- Statistics gathered by the embedded RMON agent on the switch.
- Statistics on any optional Fast Ethernet or Gigabit Ethernet HSIM or VHSIM installed in the device.

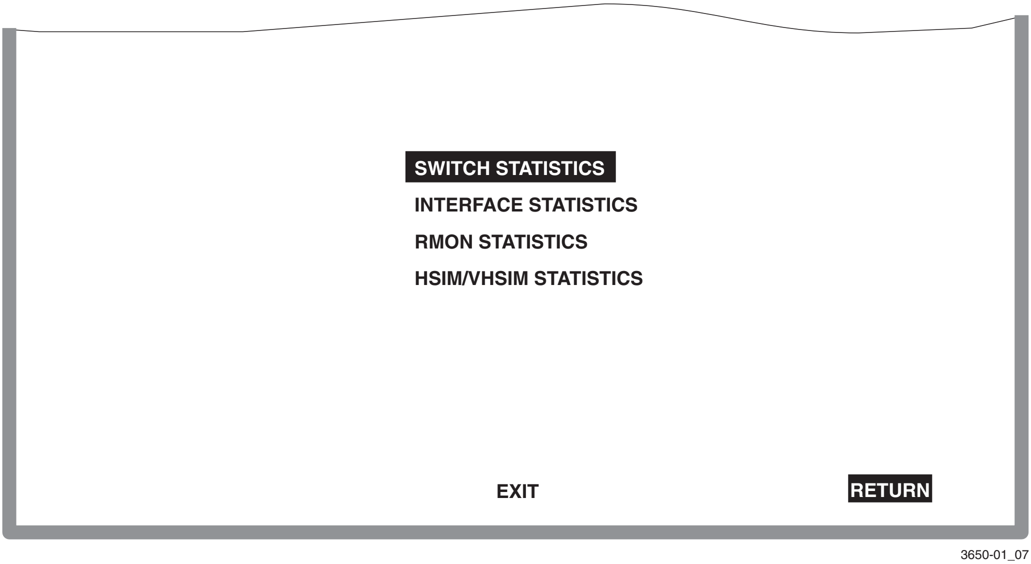
NOTE: An HSIM or VHSIM Statistics menu item does not display for non-Ethernet HSIMs or VHSIMs. If a non-Ethernet HSIM or VHSIM is installed, refer to its user's guide for more information.

How to Access

Use the arrow keys to highlight the **DEVICE STATISTICS** menu item on the Device Menu and press ENTER. The Device Statistics Menu screen, Figure 10-1, displays.

Screen Example

Figure 10-1 Device Statistics Menu Screen



Menu Descriptions

Refer to Table 10-1 for a functional description of each menu item.

Table 10-1 Device Statistics Menu Screen Menu Item Descriptions

Menu Item	Screen Function
SWITCH STATISTICS	Lists the number of frames received, transmitted, filtered, and forwarded by each switch port. For details, refer to Section 10.2.
INTERFACE STATISTICS	Provides the MIB-II statistics for each switched interface, on an interface-by-interface basis. For details, refer to Section 10.3.

Table 10-1 Device Statistics Menu Screen Menu Item Descriptions (Continued)

Menu Item	Screen Function
RMON STATISTICS	Displays all the statistics gathered by the embedded RMON agent built into the SmartSwitch device. For details, refer to Section 10.4.
HSIM/VHSIM STATISTICS	Displays the statistics screen when an optional Fast Ethernet or Gigabit Ethernet HSIM or VHSIM is installed in the device. An HSIM or VHSIM Statistics menu item does not display for non-Ethernet HSIMs or VHSIMs. If a non-Ethernet HSIM or VHSIM is installed, refer to its user’s guide for more information.

10.2 SWITCH STATISTICS SCREEN

When to Use

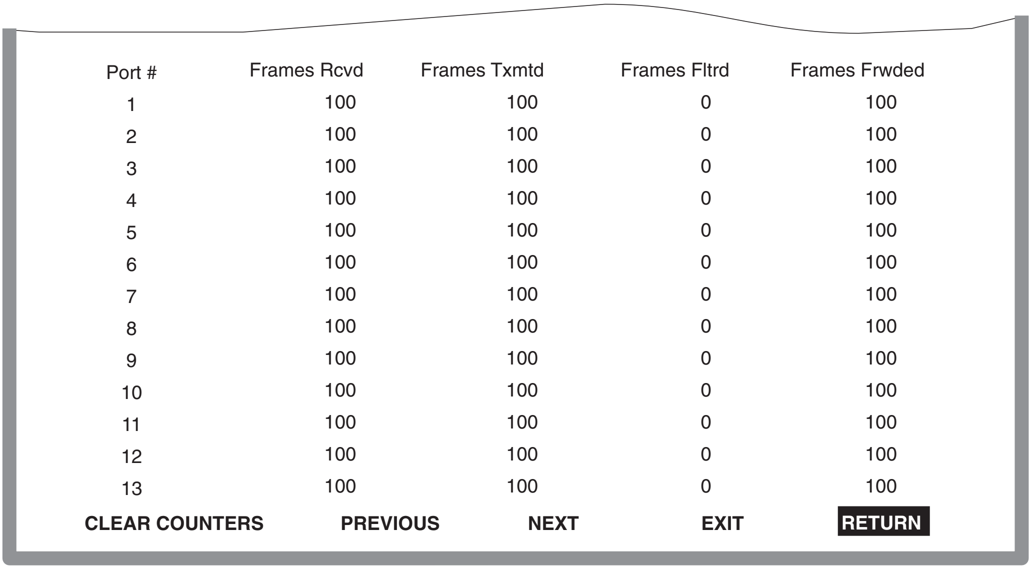
To obtain switch statistics about the number of frames received, transmitted, filtered, and forwarded by each switch port.

How to Access

Use the arrow keys to highlight the **SWITCH STATISTICS** menu item on the Device Statistics Menu screen and press ENTER. The Switch Statistics screen, Figure 10-2, displays.

Screen Example

Figure 10-2 Switch Statistics Screen



Port #	Frames Rcvd	Frames Txmtd	Frames Fltrd	Frames Frwded
1	100	100	0	100
2	100	100	0	100
3	100	100	0	100
4	100	100	0	100
5	100	100	0	100
6	100	100	0	100
7	100	100	0	100
8	100	100	0	100
9	100	100	0	100
10	100	100	0	100
11	100	100	0	100
12	100	100	0	100
13	100	100	0	100

Field Descriptions

Refer to Table 10-2 for a functional description of each screen field.

Table 10-2 Switch Statistics Screen Field Descriptions

Use this field…	To…
Port # (Read-Only)	Identify the port number. The total number of ports is dependent on the number of fixed10/100-Mbps front panel ports and the optional HSIM or VHSIM installed.
Frames Rcvd (Read-Only)	See the number of frames received by the interface since the last power-up or reset.
Frames Txmtd (Read-Only)	See the number of frames transmitted by the interface since the last power-up or reset.
Frames Fltrd (Read-Only)	See the number of frames filtered by the interface since the last power-up or reset.

Table 10-2 Switch Statistics Screen Field Descriptions (Continued)

Use this field…	To…
Frames Frwded (Read-Only)	See the number of frames forwarded by the interface since the last power-up or reset.
CLEAR COUNTERS (Command)	Temporarily reset all counters of a screen to zero, allowing the user to observe counter activity over a period of time. For details on how to use this field, refer to Section 3.1.4.

10.3 INTERFACE STATISTICS SCREEN

When to Use

To obtain the MIB-II statistics of all the switch interfaces with the exception of an installed HSIM or VHSIM.

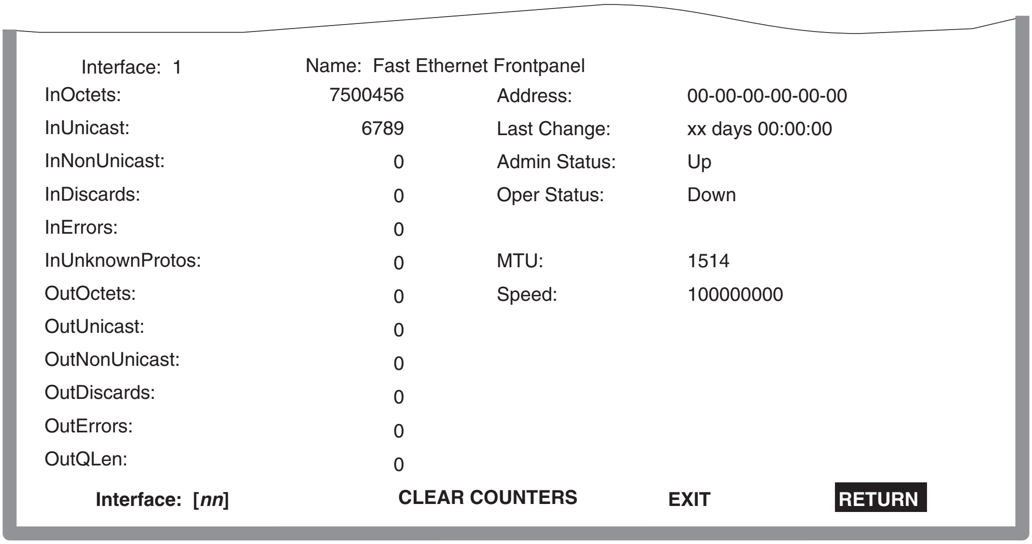
NOTE: Enterasys Networks' HSIMs that support FDDI or WAN gather their own statistics, and may be viewed via the Local Management screens of the applicable HSIM. Refer to your HSIM documentation for information on how to access these screens.

How to Access

Use the arrow keys to highlight the **INTERFACE STATISTICS** menu item on the Device Statistics Menu screen and press ENTER. The Interface Statistics screen, Figure 10-3, displays.

Screen Example

Figure 10-3 Interface Statistics Screen



```
        Interface:  1                  Name:  Fast Ethernet Frontpanel
    InOctets:                     7500456        Address:           00-00-00-00-00-00
    InUnicast:                       6789        Last Change:       xx days 00:00:00
    InNonUnicast:                       0        Admin Status:      Up
    InDiscards:                         0        Oper Status:       Down
    InErrors:                           0
    InUnknownProtos:                    0        MTU:               1514
    OutOctets:                          0        Speed:             100000000
    OutUnicast:                         0
    OutNonUnicast:                      0
    OutDiscards:                        0
    OutErrors:                          0
    OutQLen:                            0

        Interface:  [nn]              CLEAR COUNTERS        EXIT             RETURN
```

30691_54

Field Descriptions

Refer to Table 10-3 for a functional description of each screen field.

Table 10-3 Interface Statistics Screen Field Descriptions

Use this field…	To…
Interface (Read-Only)	See the Interface number for which statistics are currently being displayed. Figure 10-3 shows the Interface field displaying 1. This represents Port 1 of the device. To view other interface statistics, refer to Section 10.3.1.
Name (Read-Only)	See the type of interface for which statistics are being displayed.
InOctets (Read-Only)	See the total number of octets (bytes) that have been received on the Interface. This includes all octets including bad frames, and framing characters.

Table 10-3 Interface Statistics Screen Field Descriptions (Continued)

Use this field…	To…
InUnicast (Read-Only)	See the total number of frames that have been received that were sent to a single address.
InNonUnicast (Read-Only)	See the total number of frames that have been received that were delivered to a broadcast or multicast address.
InDiscards (Read-Only)	See the total number of inbound frames that were discarded, even though the frames contained no errors. This field may increment because the device was receiving frames during initialization and was not ready to forward them, or the switch was being overutilized.
InErrors (Read-Only)	See the total number of inbound frames that have been discarded because they contained errors. This field represents the total number of errored frames, regardless of the cause of the error.
InUnknownProtos (Read-Only)	See the total number of frames that were discarded because the frames were in an unknown or unsupported format.
OutOctets (Read-Only)	See the total number of octets (bytes) that have been transmitted from the Interface.
OutUnicast (Read-Only)	See the total number of frames transmitted that were sent to a single address.
OutNonUnicast (Read-Only)	See the total number of frames transmitted to a broadcast or multicast address.
OutDiscards (Read-Only)	See the total number of outbound frames that were discarded, even though the frames contained no errors. This field may increment, because the switch was being overutilized.
OutErrors (Read-Only)	See the total number of outbound frames discarded because they contained errors. This field represents the total number of errored frames, regardless of the cause of the error.
OutQLen (Read-Only)	See the length of the frames queue. The field represents the total number of frames that can be contained in queue.
Address (Read-Only)	See the MAC address of the interface that is currently being displayed.

Table 10-3 Interface Statistics Screen Field Descriptions (Continued)

Use this field…	To…
Last Change (Read-Only)	See the last time that the interface was reset.
Admin Status (Read-Only)	See the current status of the interface. If this field displays “Testing”, no frames may be passed on this interface.
Oper Status (Read-Only)	See the current status of the interface. If this field displays “Testing”, no frames may be passed on this interface.
MTU (Read-Only)	See the maximum frame size (in octets) that a frame may contain to be received or transmitted from this interface.
Speed (Read-Only)	See the theoretical maximum of the interface’s bandwidth in bits per second.
Interface [*nn*] (Command)	Enter an interface number for viewing statistics. For instructions on how to use this command, refer to Section 10.3.1.
CLEAR COUNTERS (Command)	Temporarily reset all counters of a screen to zero to allow the user to observe counter activity over a period of time. For details on how to use this field, refer to Section 3.1.4.

10.3.1 Displaying Interface Statistics

To display the statistics for any interface, proceed as follows:

1. Use the arrow keys to highlight the **Interface [*nn*]** field at the bottom of the screen.
2. Press the SPACE bar to increment (or press the DEL [delete] key to decrement) the interface number.
3. Press ENTER (neither the **Interface #** fields nor the statistics will change until ENTER is pressed).

10.4 RMON STATISTICS SCREEN

When to Use

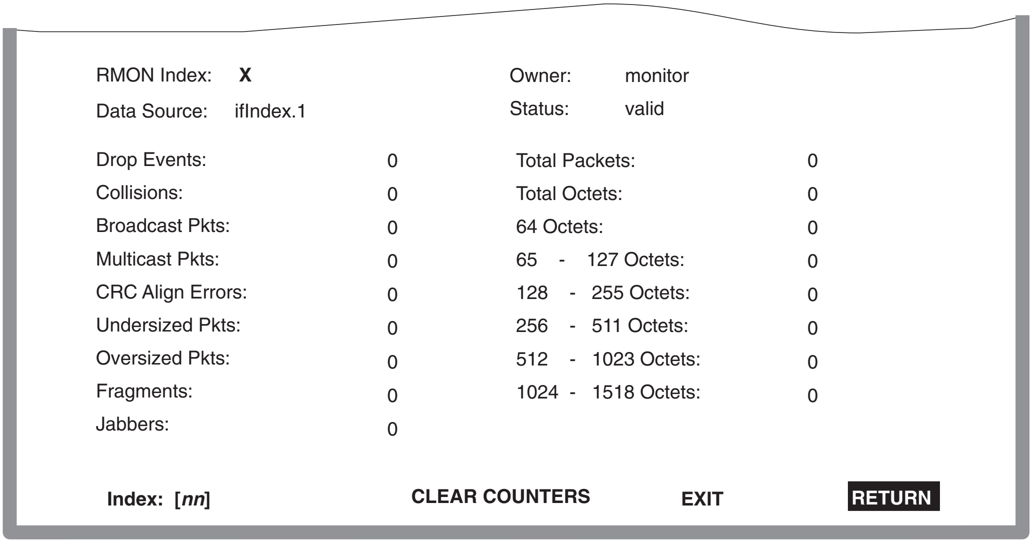
To obtain RMON statistics for each interface, on an interface-by-interface basis.

NOTE: The RMON Statistics screen provides statistics for all front panel Ethernet Interfaces, and any Ethernet HSIM/VHSIM installed in the SmartSwitch device.

How to Access

Use the arrow keys to highlight the **RMON STATISTICS** field on the Device Statistics Menu screen and press ENTER. The RMON Statistics screen, Figure 10-4, displays.

Figure 10-4 RMON Statistics Screen



```
RMON Index:   X                         Owner:       monitor
Data Source:  ifIndex.1                 Status:      valid

Drop Events:              0              Total Packets:              0
Collisions:               0              Total Octets:               0
Broadcast Pkts:           0              64 Octets:                  0
Multicast Pkts:           0              65   -  127 Octets:         0
CRC Align Errors:         0              128  -  255 Octets:         0
Undersized Pkts:          0              256  -  511 Octets:         0
Oversized Pkts:           0              512  -  1023 Octets:        0
Fragments:                0              1024 -  1518 Octets:        0
Jabbers:                  0

 Index:  [nn]            CLEAR COUNTERS         EXIT            RETURN
```

30691_55

Field Descriptions

Refer to Table 10-4 for a functional description of each screen field.

Table 10-4 RMON Statistics Screen Field Descriptions

Use this field…	To…
RMON Index (Read-Only)	See the current Ethernet interface for which statistics are being shown. The SmartSwitch device has an embedded RMON agent that gathers statistics for each interface on the device.
Data Source (Read-Only)	See the source of the statistics data that is currently being displayed on the screen. Figure 10-4 shows that the data source for this RMON index is Port 1 by displaying the name IfIndex.1. If the screen was displaying RMON statistics for Port 4, the name displayed would be IfIndex.4.
Owner (Read-Only)	See the name of the entity that configured this entry.
Status (Read-Only)	See the current operating status of the displayed interface. This field displays “valid” or “invalid”.
Drop Events (Read-Only)	See the total number of times that the RMON agent was forced to discard frames due to the lack of available switch resources. **NOTE:** The Drop Events field does not display the number of frames dropped, it only displays the number of times that the RMON agent was forced to discard frames.
Collisions (Read-Only)	See the total number of collisions that have occurred on this interface.
Broadcast Pkts (Read-Only)	See the total number of good frames that were directed to the broadcast address. The value of this field does not include multicast frames.
Multicast Pkts (Read-Only)	See the total number of good frames received that were directed to a multicast address. The value of this field does not include frames directed to the broadcast address.
CRC Align Errors (Read-Only)	See the number of frames with bad Cyclic Redundancy Checks (CRC) received from the network. The CRC is a 4-byte field in the data frame that ensures that the data received is the same as the data that was originally sent.
Undersized Pkts (Read-Only)	See the number of frames received whose size was less than the minimum Ethernet frame size of 64 bytes, not including preamble, but have a valid CRC.

Table 10-4 RMON Statistics Screen Field Descriptions (Continued)

Use this field…	To…
Oversized Pkts (Read-Only)	See the number of frames received whose size exceeded 1518 data bytes, not including preamble, but have a valid CRC.
Fragments (Read-Only)	See the number of received frames that are not the minimum number of bytes in length or received frames that had a bad or missing Frame Check Sequence (FCS), were less than 64 bytes in length (excluding framing bits, but including FCS bytes), and have an invalid CRC. **NOTE:** It is normal for the Fragments field to increment. Fragments are a normal result of collisions in a half-duplex network.
Jabbers (Read-Only)	See the total number of frames that were greater than 1518 bytes and had either a bad FCS or a bad CRC.
Total Packets (Read-Only)	See the total number of frames (including bad frames, broadcast frames, and multicast frames) received on this interface.
Total Octets (Read-Only)	See the total number of octets (bytes) of data, including those in bad frames, received on this interface.
64 Octets (Read-Only)	See the total number of frames, including bad frames, received that were 64 bytes in length (excluding framing bits, but including FCS bytes).
65 – 127 Octets (Read-Only)	See the total number of frames, including bad frames, received that were between 65 and 127 bytes in length (excluding framing bits, but including FCS bytes).
128 – 255 Octets (Read-Only)	See the total number of frames, including bad frames, received that were between 128 and 255 bytes in length (excluding framing bits, but including FCS bytes).
256 – 511 Octets (Read-Only)	See the total number of frames, including bad frames, received that were between 256 and 511 bytes in length (excluding framing bits, but including FCS bytes).
512 – 1023 Octets (Read-Only)	See the total number of frames, including bad frames, received that were between 512 and 1023 bytes in length (excluding framing bits, but including FCS bytes).

Table 10-4 RMON Statistics Screen Field Descriptions (Continued)

Use this field…	To…
1024 – 1518 Octets (Read-Only)	See the total number of frames, including bad frames, received that were between 1024 and 1518 bytes in length (excluding framing bits, but including FCS bytes).
Index [*nn*] (Command)	Enter a port number to view its statistics. For instructions on how to use this command, refer to Section 10.4.1.
CLEAR COUNTERS (Command)	Temporarily reset all counters of a screen to zero to allow the user to observe counter activity over a period of time. For details on how to use this command, refer to Section 3.1.4.

10.4.1 Displaying RMON Statistics

To display the statistics for any index, proceed as follows:

1. Use the arrow keys to highlight the **Index [*nn*]** field at the bottom of the screen.
2. Press the SPACE bar to increment (or press the DEL [delete] key to decrement) the index number (number of the port interface).
3. Press ENTER (neither the **RMON Index** field nor the statistics will change until ENTER is pressed). The RMON interface index of statistics for the port is displayed.

11

Network Tools Screens

This chapter describes the Network Tools Help screen and how to use it and the Network Tools commands to access and manage network devices. An example of each command is also included.

Screen Navigation Paths

Password > Device Menu > **Network Tools**

11.1 NETWORK TOOLS

When to Use

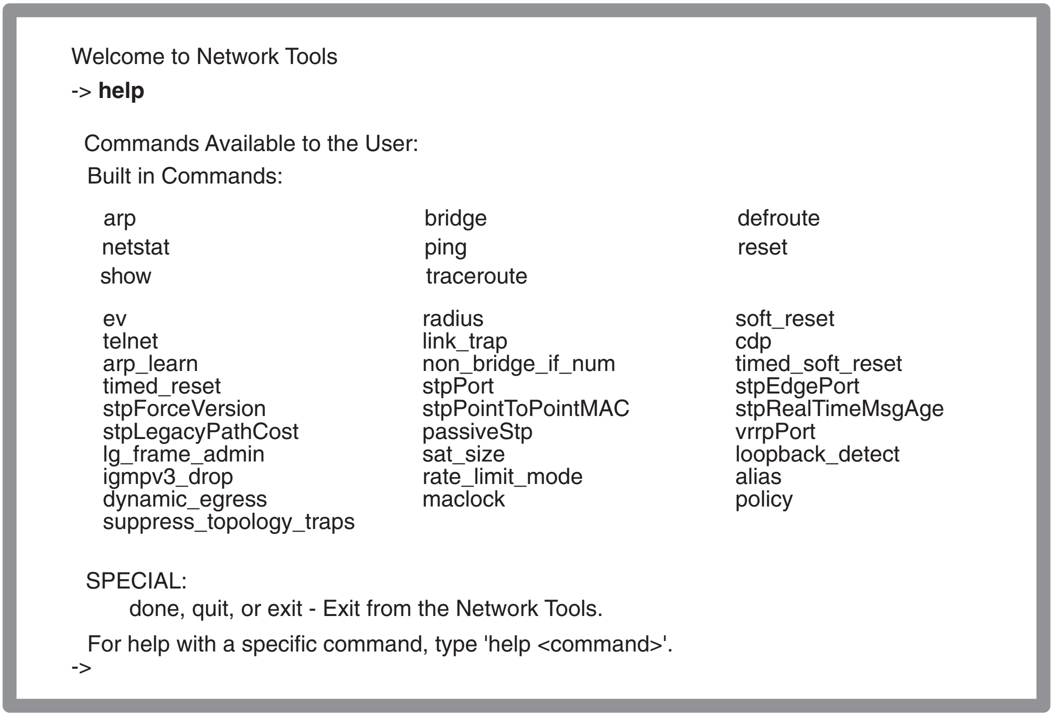
To access and manage network devices using the Network Tools command set.

How to Access

Use the arrow keys to highlight the **NETWORK TOOLS** menu item in the Device Menu screen and press ENTER. The Network Tools Help screen, Figure 11-1, displays.

TIP: Type **help** at the prompt to list all the commands that are available in the current operational mode. A command used incorrectly (wrong syntax) will prompt a display of the correct usage. Use lowercase characters when entering commands in Network Tools.

Screen ExampleNetwork Tools Help Screen



```
Welcome to Network Tools
-> help

  Commands Available to the User:
  Built in Commands:

    arp                          bridge                       defroute
    netstat                      ping                         reset
    show                         traceroute

    ev                           radius                       soft_reset
    telnet                       link_trap                    cdp
    arp_learn                    non_bridge_if_num            timed_soft_reset
    timed_reset                  stpPort                      stpEdgePort
    stpForceVersion              stpPointToPointMAC           stpRealTimeMsgAge
    stpLegacyPathCost            passiveStp                   vrrpPort
    lg_frame_admin               sat_size                     loopback_detect
    igmpv3_drop                  rate_limit_mode              alias
    dynamic_egress               maclock                      policy
    suppress_topology_traps

  SPECIAL:
      done, quit, or exit - Exit from the Network Tools.

  For help with a specific command, type 'help <command>'.
->
```

36502_02

The Network Tools functions are performed using a series of commands. Entering commands in Network Tools involves typing the command to be executed at the Network Tools prompt, adding any desired or required extensions, and pressing ENTER.

There are two categories of commands in the command set: Built-in and Special, which are described below and detailed in Sections 11.2 and 11.5.

- Built-in Commands – Allow you to access and manage network devices.

NOTE: The atm_stp_state command only displays when an HSIM or VHSIM is installed that supports ATM, such as the HSIM-A6DP or VHSIM2-A6DP.

Refer to Table 11-1 for a list of the commands.

Table 11-1 Built-In Commands

alias	arp	arp_learn	atm_stp_state[1]
bridge	cdp	defroute	dynamic_egress
ev	gigabit_port_mode[2]	igmpv3_drop	lg_frame_admin
link_trap	loopback_detect	maclock	netstat
non_bridge_if_num	passiveStp	ping	policy
radius	rate_limit_mode	reset	sat_size
show	soft_reset	stpEdgePort	stpForceVersion
stpLegacyPathCost	stpPointToPointMAC	stpPort	stpRealTimeMsgAge
suppress_topology_traps	telnet	timed_soft_reset	timed_reset
traceroute	vrrpPort		

[1] The atm_stp_state command only displays when an HSIM or VHSIM is installed that supports ATM, such as the HSIM-A6DP or VHSIM2-A6DP.

[2] The gigabit_port_mode command only displays when a gigabit interface module is installed.

- Special Commands – Allow the user to exit from Network Tools. The commands are done, quit, and exit.

NOTES: The conventions used in describing the commands in Network Tools are as follows:

Arguments enclosed by [ ] are required.

Arguments enclosed by < > are optional.

In the following command examples, the information entered by the user is shown in **bold** font.

To abort the output or interrupt a process, press the CONTROL key and c key simultaneously, designated as ^C here.

The commands are presented in the following format:

command	
Description:	Briefly describes the command and its uses.
Syntax:	Shows the required command format. It indicates where arguments, if any, must be specified.
Options:	Lists any additional fields in the appropriate format that may be added to the command.
Example:	Shows an example of the command.

11.2 BUILT-IN COMMANDS

The built-in commands listed in this section activate functions on the LM managed device or devices being accessed through Network Tools.

alias	
Description:	Enables, disables and configures alias snooping on a per-port basis.
Syntax:	**alias [enable | disable | status] [ALL | port # | port range, i.e., 1-5]** **alias [stats]** **alias [clear_stats]** **alias [fwd_list]** **alias [fwd_set] [rate | burst] [value]**
Options:	**enable** – Enables alias snooping on specific port or port range. **disable** – Disables alias snooping on specified ports or port range **status** – Displays the current alias snooping state (enabled or disabled) on a port or port range. **stats** – Displays current alias snooping state statistics. **clear_stats** – Clears all alias snooping statistics. **fwd_list** – Lists current configuration settings including max frame size, max host queue, max PPS, and max burst. **fwd_set** – Allows setting of max PPS and/or max burst configuration settings.

alias (Continued)

Examples:

```
-> alias disable 1-4
Snooping is disabled on port 1.
Snooping is disabled on port 2.
Snooping is disabled on port 3.
Snooping is disabled on port 4.
-> alias status 1
Snooping is disabled on port 1.
-> alias stats
Pkts Sent [    <= 64]: 0
Pkts Sent [ 65...128]: 0
Pkts Sent [129...256]: 0
Pkts Sent [257...512]: 0
Pkts Sent [512..1024]: 0
Pkts Sent [   > 1024]: 0
Pkts Dropped (Q full): 0
Pkts Dropped   (Rate): 0
Pkts Truncated       : 0
Port State Deltas    : 93
Port State No Change : 0
Host Enqueue Drop    : 0
Host Enqueue Success : 0
Host Bad Release Cnt : 0
-> alias fwd_list
Max Frame Size      :  1500
Max Host Queue Usage:  32
Max PPS             :  100
Max Burst           :  64
-> alias fwd_set rate 200
Max Frame Size      :  1500
Max Host Queue Usage:  32
Max PPS             :  200
Max Burst           :  64
```

arp

Description:

Provides access to the ARP (Address Resolution Protocol) cache, enabling you to view cache data, delete entries, or add a static route. Super-user access is required to delete an entry or add a static route.

Each ARP cache entry lists the network *interface* that the switch module is connected to, the device's *network address* or IP address, the device's *physical address* or MAC address, and the *media type* of connection to the device. Media types display as numbers, which stand for the following states:

1 – Other

2 – Invalid entry (cannot ping device, timed out, etc.)

3 – Dynamic route entry

4 – Static route entry (not subject to change)

You must specify the arp command with one of the options specified in this table.

Syntax: **arp <options>**

Options:

-a – Views cache data

-d – Deletes an IP address entry. Requires additional arguments: [Interface Number] [IP address]

-s – Adds a static entry. Requires additional arguments: [Interface Number] [IP address] [MAC address]

-f – Flushes the ARP cache

Examples:

```
-> arp-a

#interface     Network Address     Physical Address       Media Type
#30            122.144.40.111      00.00.0e.12.3c.04      3(dynamic)
#30            122.144.48.109      00.00.0e.13.3d.14      3(dynamic)
#30            122.144.52.68       00.00.0e.12.3c.04      3(dynamic)
#30            122.144.21.43       00.00.0e.03.1d.3c      3(dynamic)

-> arp-d 1 122.144.52.68

-> arp-s 1 22.44.2.3 00:00:0e:1d:3c

-> arp-f
```

arp_learn

Description: Sets how the ARP cache entry will be affected under different conditions as described in the options below, and displays current ARP cache settings.

Syntax: **arp_learn [normal | limited | status]**

Options:

normal – Changes the ARP cache entry for a given IP Address, if the source address (SA) in the entry does not match that of any received IP Packet.

limited – Causes the ARP entry to change only by ARP request and ARP response packets. Other IP packets will be ignored.

status – Displays the current status information about ARP Cache.

Example:

```
-> arp_learn status
Current ARP Cache Learn status: NORMAL
-> arp_learn limited
Setting ARP Cache Learning to LIMITED.
!! Don't forget to set a Default Gateway !!
-> arp_learn normal
Setting ARP Cache Learning to NORMAL.
```

bridge

Description: Enables or disables one or more bridge interfaces, either one at a time or all at once.

Syntax: **bridge [ENABLE/DISABLE] [IFNUM/ALL]**

Options:

ENABLE/DISABLE — Enables or disables specified bridge interfaces.

IFNUM/ALL — Specifies a bridge interface number or all bridge interfaces.

Example:

```
-> bridge disable all
-> bridge enable 1
-> bridge disable 1
```

cdp

Description: Enables, disables or displays the status of the CDP Discovery Protocol.

Syntax: **cdp [enable/disable/status**]

Options:

enable — Enables CDP discovery protocol on the device.

disable — Disables CDP discovery prototol on the device.

status — Displays the status of the CDP discovery protocol.

Examples:

```
-> cdp status
CDP is Enabled

-> cdp disable

-> cdp status
CDP is Disabled
```

defroute

Description: Displays, sets, or deletes the default IP route to a managed device through the specified interface.

Syntax:

defroute

defroute [interface number] [IP address]

defroute delete [interface number] [IP address]

Options:

interface number — Specifies the default IP route interface number.

IP address — Specifies the default IP route IP address.

Examples:

```
-> defroute

   # Default route is 147.152.42.32 on interface 2

-> defroute 2 147.152.42.32

   # Default route is 147.152.42.32 on interface 2

-> defroute delete

   # Default route is not currently set.
```

dynamic_egress

Description: Enables, disables or displays the status of the dynamic_egress control function. The command requires a corresponding VLAN Identifier (VID).

The dynamic_egress control function allows or disallows VLANs to be dynamically added to the dynamic Port VLAN Lists of a port. The default is that no dynamic Port VLAN Lists will be modified. The lists are modified based on the inbound traffic on a port. After a frame is classified into a VLAN (via PVID, L2/L3/L4 classification, etc.), that VLAN is added to the dynamic Port VLAN List of that port. The following three conditions must be met before the VLAN is added to the dynamic Port VLAN List.

1. The feature is enabled for that VLAN.
2. The frame was not Q-tagged (priority tagged or untagged is okay).
3. The SmartSwitch device is not currently in STP blocking or listening on that port.

After a VLAN has been added to the dynamic Port VLAN List, the entry is subject to time out (age out) if the port does not receive another frame for that VLAN within the aging time. The dynamic-egress aging time is equal to the Spanning Tree aging time (default is 300 seconds).

NOTE: Devices that do not source frames regularly (such as printers), may not operate properly with dynamic egress enabled. In these cases, it is recommended to manually create Port VLAN Lists.

For an example of how dynamic_egress functions, refer to Section 11.3.

Syntax: **dynamic_egress [action] [vid]**

Options: **action:**

status – Allows the status of the dynamic_egress function to be checked to see if it is enabled or disabled.

enable – Allows dynamic egress modification for the vid.

disable – Disallows dynamic egress modification for the vid.

vid:
The VID of the VLAN to be acted on. The VLAN must be one that has been configured in the switch before it can be selected. The maximum VID value that can be entered is 4095.

dynamic_egress (Continued)

Examples:

```
-> dynamic_egress status 1

Dynamic Egress Disabled for VLAN ID 0x0001

-> dynamic_egress enable 1

Dynamic Egress Enabled for VLAN ID 0x0001

-> dynamic_egress disable 1

Dynamic Egress Disabled for VLAN ID 0x0001
```

ev

Description: Enables or disables groups of events or all events concerning logging functions.

Syntax: **Enable [Group]**

Disable [Group] [Trap] [#|ALL]

Commands to Control Logging Functions:

ev STARt [Logging] [Trapping] – begin logging events/

ev STOp [Logging] [Trapping] – stop logging events/trap

ev Clear – clear the log

ev SEverity <severity level> – set/show current logging severity

ev filter [get | set <string>] – get/set search string

ev logsize [get|set <#(50-5000)>] – get/set dynamic log buffer size

Commands for Listing Events:

ev List [ENabled] [GROUPS|Traps|EVents|Log] – list various items

If the argument enabled is used, then only the enabled events, traps, or groups are listed.

ev List GROUP_Event # – list events for group #

Commands for Miscellaneous Log/Event Functions:

ev STus – status of log system

ev SCreensize [#] – set # of listed events/screenful#

ev (Continued)

Options:

ENABLE – Enables Group or events or all

DISABLE – Disables Group or events or all

Commands to Control Logging Functions:

ev STARt [Logging] [Trapping] – begin logging events/traps

ev STOp [Logging] [Trapping] – stop logging events/traps

ev Clear – clear the log

ev SEverity <severity level> – set/show current logging severity

ev filter [get | set <string>] – get/set search string

ev logsize [get|set <#(50-5000)>] – get/set dynamic log buffer size

Commands for Listing Events:

ev List [ENabled] [GROUPS|Traps|EVents|Log] – list various items

If the argument enabled is used, then only enabled events
or traps or groups are listed.

ev List GROUP_Event # – list events for group #

Commands for Miscellaneous Log/Event Functions:

ev STus – status of log system

ev SCreensize [#] – set # of listed events/screenful#

Example:

```
-> ev disable all
logging(E) - Trapping(D) - Trapped(F) - LogWrapped - #logged
(4/4)
```

gigabit_port_mode

Description: Configures or displays the status of Gigabit Ethernet ports. Changing the mode will cause a reset and loss of all data in NVRAM with the exception of the IP Address and Subnet IP Address.

NOTE: This field is displayed only when the switch module supports an installed Gigabit Ethernet VHSIM.

Syntax: **gigabit_port_mode [active | redundant | status]**

Options:

active – Enables both gigabit ports.

redundant – Causes Port 1 to be active and Port 2 to be set up as a redundant port.

status – Displays the current status of the gigabit port.

Examples:

```
-> gigabit_port_mode status

gigabit_port_mode is redundant

-> gigabit_port_mode active

This will reset board and cause loss of persistent objects
except IP Address and Subnet: Are you *SURE* ?
```

igmpv3_drop

Description: Enables, disables or displays the status of igmpv3_ drop on Ethernet front panel ports.

Syntax: **igmpv3_drop [enable | disable | status]**

Options:

enable — Enables igmpv3 drop on Ethernet front panel ports. This is the device default state.

disable — Disables igmpv3 drop on Ethernet front panel ports.

status — Displays the current state of igmpv3_drop on the device.

Examples:

```
-> igmpv3_drop enable

-> igmpv3_drop disable

-> igmpv3_drop status

igmpv3 drop is Disabled.
```

lg_frame_admin

Description: Enables large frame support on a per port basis. allowing the user to determine if large frames can be forwarded out a particular port.

Syntax: **lg_frame_admin [set] [LARGE | FRAG_IF_POSS | SMALL | AUTO] [PORT | ALL_BPLANE | ALL_FDDI]**

lg_frame_admin [status] [port #]

Options: **set** – Sets the size of transmitted frames for a port or a group of ports.

status – Causes the display of the current settings for one port or a group of ports (e.g., 1– 15).

LARGE – Sets the port to allow all valid large frames to be transmitted out the port.

FRAG_IF_POSS – This is a special setting. Sets the port, so that all large IP frames that can be fragmented will be fragmented before being transmitted out the port. If the large frame cannot be fragmented, then it will be transmitted out the port as a large frame.

SMALL – Sets the port so that frames will be transmitted as either fragmented (if possible), or dropped if they cannot be fragmented.

AUTO – Same as SMALL.

PORT – Enables the mib II port number to change the settings.

ALL_BPLANE – Causes all the backplane ports to have the same setting.

ALL_FDDI – Causes all FDDI HSIMs to have the same setting.

NOTE: Only backplane and FDDI HSIMs can be configured beyond the default settings.

Examples:

```
-> lg_frame_admin set FRAG_IF_POSS all_bplane

The Status for large interfaces has been changed to
FRAG_IF_POSS on all BACK PLANE interfaces.

-> lg_frame_admin status 19

Large frame port status is FRAG_IF_POSSAUTO on Port 19.
```

link_trap

Description: Enables, disables, or displays the status of link traps on one or all ports.

Syntax: **link_trap [enable/disable/status] <PORT/all>**

Options:

enable — Enables a link trap.

disable — Disables a link trap.

status — Displays link trap status.

PORT/ all — Specifies a port or all ports.

Examples:

```
-> link_trap status
LINK TRAP STATUS:
   Port 1  is ENABLED         Port 2  is DISABLED
   Port 3  is ENABLED         Port 4  is ENABLED
-> link_trap disable 2
Link traps have been DISABLED on port 2
-> link_trap disable all
Link traps have been DISABLED on all ports (1-24)
-> link_trap status 3
Link traps are ENABLED on port 3
```

loopback_detect

Description: Enables, disables, or displays the status of loopback detection on Ethernet front panel ports.

Syntax: **loopback_detect [enable | disable | state]**

Options:

enable – Enables loopback detection on Ethernet front panel ports.

disable – Disables loopback detection on Ethernet front panel ports.

state – Indicates if loopback detection is enabled or disabled.

loopback_detect (Continued)

Examples:

```
-> loopback_detect enable
-> loopback_detect disable

-> loopback_detect state

Loopback_detect is disabled.
```

maclock

Description: Configures the MAC locking feature per port. When enabled, either a static MAC is locked to the port, or the first MAC seen on the port is locked to that port. Only incoming traffic with the locked MAC as the source MAC address shall be forwarded. If traps are enabled, then the first MAC that differs from the locked MAC is sent as a trap to management.

Syntax: **maclock show [port# | all]**

Displays the status of MAC locking globally or on one or more ports, as well as whether or not MAC lock trap messaging is enabled or disabled, the maximum static and end station MAC addresses allowed locked to each port, and any MAC address(es) violating the maximum static and first arrival value(s) set for each port.

maclock show stations [port# | all] [firstarrival [port# | all]] [static [port# | all]]

Displays MAC locking information about first arrival, static (management defined) or all end stations connected to the device.

maclock (Continued)

Syntax: (Continued)

maclock set enable [port# | all | global]

Enables MAC locking globally or on one or more ports. When enabled and configured for a specific MAC address and port string, this locks a port so that only one end station address is allowed to participate in frame relay.

maclock set disable [port# | all | global]

Disables MAC locking globally or on one or more ports.

maclock set <macaddress> < port# | all > < create | enable | disable>

Creates a static MAC address and enables or disables MAC locking for the specified MAC address and port. When created and enabled, this allows only the end station designated by the MAC address to participate in frame relay.

maclock set firstarrival < port# | all > < value >

Restricts MAC locking on a port to a maximum number of end station addresses first connected to that port.

maclock set static < port# | all > < value >

Restricts MAC locking on a port to a maximum number of static (management defined) MAC addresses for end stations connected to that port. Valid values are 0 to 20.

maclock set trap < port# | all > < enable | disable >

Enables or disables MAC lock trap messaging globally or one one or more ports. When enabled, this authorizes the device to send an SNMP trap message if an end station is connected that exceeds the maximum values configured using the **maclock set firstarrival** and **maclock set static** commands. Violating MAC addresses are dropped from the device’s routing table.

maclock clear static < port# | all >

Clears statically configured MAC locking entries from one or more ports.

maclock clear <macaddress> < port# | all >

Clears a MAC locking entry from one or more ports.

maclock (Continued)

Options:

port# | all — Applies MAC locking parameters to a specific ports or to all ports on the device.

global — Applies MAC locking parameters globally.

firstarrival — Displays MAC locking information about first arrival end stations connected to the device.

static — Displays MAC locking information about managment defined end stations connected to the device.

Examples:

```
-> maclock show
MAC locking is globally enabled


  Port     Port     Trap     Max Static  Max FirstArrival      Violating
 Number   Status   Status    Allocated     Allocated          MAC Address
________ ________ ________  ____________ ________________   ________________
   1     Disabled Disabled        1             10
   2     Disabled Disabled        2             20
   3     Disabled Disabled        3             30
   4     Disabled Disabled        4             40
   5     Disabled Disabled        5             50
   6     Disabled Disabled       20            600
   7     Enabled  Disabled        1              1           00:00:1D:B1:10:F3
   8     Disabled Disabled       20            600
   9     Disabled Disabled       20            600
----- More -----
-> maclock show stations
Port Number     MAC Address              Status            State
___________     ___________________    _____________    _______________
   7             00:00:1D:B1:11:01      Active          first learned
```

maclock (Continued)

Examples: (Continued)

```
-> maclock set enable global
MAC locking is globally enabled.
-> maclock set disable global
MAC locking is globally disabled.
-> maclock set 00:a0:c9:0d:32:11 3 create
MAC_locking for MAC 00:A0:C9:0D:32:11 created on Port 3.
-> maclock set firstarrival 3 6
MAC-Locking Dynamic entry changed to 6 on port  3.
-> maclock set static 3 4
MAC-Locking Static entry changed to 3 on port 4.
-> maclock settrap 3 enable
Enabling MAC-Locking traps on Port 3.
-> maclock clear static 3
Statically locked MACs cleared on port 3.
-> maclock clear 00:a0:c9:0d:32:11 3
MAC 00:A0:C9:0D:32:11 cleared from Port 3.
```

netstat

Description: Displays general network statistics for the managed device.

Syntax: **netstat [option]**

Options:

-i – Displays status and capability information for each interface.

-r – Displays routing information for each interface.

netstat (Continued)

Example:

```
-> netstat -i
Interface + DescriptionMTU  Speed    Admin Oper MAC Addr

#1 (ethernet - csmacd) 1514 10000000 up    up   0x00 0x00 0x1d 0x07 0x50 0x0e
#2 (ethernet - csmacd) 1514 10000000 up    up   0x00 0x00 0x1d 0x07 0x50 0x0f
#3 (ethernet - csmacd) 1514 10000000 up    up   0x00 0x00 0x1d 0x07 0x50 0x10
#4 (ethernet - csmacd) 1514 10000000 up    up   0x00 0x00 0x1d 0x07 0x50 0x11

-> netstat -r
Destination              Next-hop         Interface

# Default Route          DirectConnection 1
# 134.141.0.0            DirectConnection 2
# 134.141.0.0            DirectConnection 3
```

non_bridge_if_num

Description: Configures or displays the current interface number assigned to non-bridge ports. Changing of the interface number assigned to non-bridge ports will lead to a reset of the board.

Syntax: **non_bridge_if_num [0 | 9999 | status]**

Options: **0 | 9999** — Specifies an interface number.

status — Displays the non-bridge interface number.

Example:

```
-> non_bridge_if_num_status
non bridge interface number is 0.
```

passiveStp

Description: Enables, disables, or displays the status of Passive Mode Spanning Tree on the device.

Passive Mode Spanning tree allows ports on leaf bridges to transition very quickly and not invoke a global network re-span through requesting root elections by:

- Not allowing switches to become the root node;
- Not allowing switches to send configuration BPDUs;
- Expiring the message age timer when a link transitions to a down state;
- Moving the 802.1D Blocked state directly to forwarding; and
- Using a default or locally defined Passive STP Max Age time.

Syntax: **passiveStp [enable | disable | status]**

Options: **enable** – Enables PassiveStp on this device.

disable – Disables PassiveStp on this device.

status – Indicates the current status of Passive STP.

Examples:

```
->PassiveStp disable
Disabled
->PassiveStp status
Passive is disabled
Passive Maxage = 2000
```

ping

Description: Generates an outbound ping request to check the status (alive/not alive) of a device at a specified IP address.

Syntax: **ping [IP address]**

Options: **IP address** — Specifies the IP address to ping.

Example:

```
-> ping 122.144.40.10
122.144.40.10 is alive
```

policy

Description: Displays the policy table and configures policy-port mappings.

Syntax: **policy show profile <profile_index>**

Displays the policy table, including policy index, policy name, policy status (enable/disable), and PVID and priority override information

policy show port <port_number_or_range_or_all>

Displays the policy status of one or more ports, including default policy, current policy, authentication type (Static, PWA, EAP and MAC), authentication status (Auth/NoAuth/NA) and authentication information (authenticated MAC or UserName).

policy set port <port_number_or_range_or_all> <profile_index>

Maps a policy statically to one or more ports.

policy clear profile port <port_number_or_range_or_all>

Unmaps a policy statically from one or more ports.

Options: **profile_index** — Specifies the profile index assigned to a policy.

port_number_or_range_or_all — Displays or configures policies for a specific port, a range of ports, or all ports on the device.

Examples:

```
-> policy show profile 1-5
-------------------------------------------------------------------------------
Index  Name      Status    PVID          PVIDStatus  PRI    PRIStatus
-------------------------------------------------------------------------------
1      Default   Enable    1             Enable      0      Disable
2      Employee  Enable    2             Enable      1      Enable
3      Guest     Enable    3             Enable      0      Disable
4      Admin     Enable    4             Enable      7      Enable
5      Test      Disable   1             Disable     0      Disable
```

policy (Continued)

Examples:
(Contiued)

```
-> policy show port 1-4
------------------------------------------------------------------------------
Port   DefaultPolicy  CurrentPolicy  AuthType  AuthStatus   AuthInfo
------------------------------------------------------------------------------
1      Guest          Guest          Static    N/A          N/A
2      Guest          Admin          MAC       Auth         00:00:1D:AA:AA:AA
3      <none>         <none>         <none>    N/A          N/A
4      Guest          Employee       EAP       Auth         john.doe
8      <none>         <none>         <none>    N/A          N/A

-> policy set port 1-2 1
------------------------------------------------------------------------------
Port   DefaultPolicy  CurrentPolicy  AuthType  AuthStatus   AuthInfo
------------------------------------------------------------------------------
1      Default        Default        Static    N/A          N/A
2      Default        Default        Static    N/A          N/A

-> policy clear profile port 1-2
------------------------------------------------------------------------------
Port   DefaultPolicy  CurrentPolicy  AuthType  AuthStatus   AuthInfo
------------------------------------------------------------------------------
1      <none>         <none>         <none>    N/A          N/A
2      <none>         <none>         <none>    N/A          N/A
```

radius

Description: Enables, disables, and configures RADIUS authentication, which can only be used when the client has been properly configured and enabled. When the RADIUS Client is not enabled, the legacy password authentication will run as before. For more about Radius Client, refer to Section 3.6.1.

Syntax:

radius

radius status

radius [enable | disable]

radius prim_ip <server ip>

radius sec_ip <server ip>

radius prim_ip <server ip>

radius sec_ip <server ip>

radius timeout <n>

radius retry <n>

radius clear

radius prim_auth_port <n>

radius sec_auth_port <n>

radius prim_acct_port <n>

radius sec_acct_port <n>

radius last_resort < [local|remote] [accept|reject|challenge] >

radius prim_secret

radius sec_secret

radius (Continued)

Options:

radius — Shows RADIUS help.

radius status — Shows all RADIUS client settings.

radius [enable | disable] — Enables or disables the RADIUS Client.

radius prim_ip <server ip> — Shows <sets> the primary RADIUS server's IP, in decimal-dotted format.

radius sec_ip <server ip> — Shows <sets> the secondary RADIUS server's IP, in decimal-dotted format.

radius timeout <n> — Shows <sets> RADIUS server timeout in seconds.

radius retry <n> — Shows <sets> number of RADIUS server retries.

radius clear — Resets all RADIUS client settings.

radius prim_auth_port <n> — Shows <sets> the primary RADIUS server's UDP authentication port.

radius sec_auth_port <n> — Shows <sets> the secondary RADIUS server's UDP authentication port.

radius prim_acct_port <n> — Shows <sets> the primary RADIUS server's UDP accounting port.

radius sec_acct_port <n> — Shows <sets> the secondary RADIUS server's UDP accounting port.

radius last_resort < [local|remote] [accept|reject|challenge] > — Shows <sets> the last-resort action to take if all RADIUS servers timeout, for either local (COM port) or remote (TELNET) sessions:

Accept – accept user with no further authentication
Reject – reject user unconditionally
Challenge – challenge the user for the system password (i.e., revert to legacy module passwords)

radius (Continued)

Options: (Cont'd)

radius prim_secret — Sets the primary RADIUS server's shared secret.

radius sec_secret — Sets the secondary RADIUS server's shared secret.

NOTES: The secret is NOT encrypted in transit; if this command is used over TELNET then the secret may be compromised.

Examples:For maximum security, it is recommend to use a 16 to 32 character string for the shared secret code. For security reasons, the entered code appears as asterisks (*) on the screen.

Examples:

```
-> radius client
RADIUS Configuration Cli
Command Format : radius
status            (shows Radius status)
clear             (clears all entries)
timeout           (server timeout, seconds)
last_resort       <local|remote> <accept|reject|challenge>
retry             <number of retry attempts>
enable            (enables radius client)
disable           (disables radius client)
prim_secret       (sets primary secret)
prim_ip           <primary server IP>
prim_auth_port    <primary server authentication port>
prim_acct_port    <primary server acct port>
sec_secret        (sets secondary secret)
sec_ip            <secondary server IP>
sec_auth_port     <secondary server authentication port>
sec_acct_port     <secondary server acct port>
```

radius (Continued)

Examples: (Cont'd)

NOTE: The following shows examples of when 3, 7, and 32 characters are entered as the secret code (16 to 32 characters are recommended).

```
-> radius sec_secret
Enter Secret (max 32): ***
Confirm Secret: ***
#  ERROR : secret minimum length is 6
-> radius sec_secret
Enter Secret (max 32): *******
Confirm Secret: *******
Warning: rfc2865 recommends min length of 16
ok
-> radius sec_secret
Enter Secret (max 32): ********************************
Confirm Secret: ********************************
ok
```

rate_limit_mode

Description: Displays the status of rate limiting or configures the exit-rate limit range to either the default high_range (100 Kbps to 1 Gbps) or the low range (50 Kbps to 400 Mbps). This mode is stored in non-volatile memory and is retained by normal resetting. Changing from one mode to the other mode may result in current settings being removed if their range is no longer valid. Changing rate limit mode will require a reset.

Syntax: **rate_limit_mode [status] [high_range (default)] [low_range]**

Options:

status — Displays rate limiting status.

high_range — Sets the default rate limit high range.

low_range — Sets the default rate limit low range.

rate_limit_mode (Continued)

Examples:

```
-> rate_limit_mode status
Rate Limit Mode is: High Range (100Kbps - 1 Gbps).
-> rate_limit_mode low_range
This will reset board : Are you *SURE* ?
-> rate_limit_mode high_range
This will reset board : Are you *SURE* ?
```

reset

Description: Initiates a hardware reset of the device. This command initializes the CPU processor, runs the onboard diagnostics, and restarts the software image, which restores the user configuration settings from NVRAM. The user will be queried to confirm the reset command to ensure against unwanted resets.

NOTE: The Network Tools connection to the device will be terminated upon execution of this command.

Syntax: **reset**

Options: None

Example:

```
-> reset
RESET: Are you *SURE
-> Y
```

sat_size

Description: Displays the current setting or sets the size of the Source Address Table (Forwarding Database) on the device to either 8000 or 16000 entries. The default is 8000 entries. When set to 16000, 400 Layer 2/3/4 VLAN Classification and Priority Assignment entries will be supported. The default is 1000 Layer 2/3/4 VLAN Classification and Priority Assignment entries. Changing of sat_size will lead to a reset of the board.

Syntax: **sat_size [8 | 16 | status]**

Options:

8 — Sets the size of the Source Address Table to 8000 entries.

16 — Sets the size of the Source Address Table to 16000 entries.

status — Displays the current size setting for the Source Address Table.

Example:

```
-> sat_size status

sat size status is 8.
```

show

Description: Displays information concerning various components of the device. Protocols currently supported are IP, IPX, DECnet, and AppleTalk. Components of those protocols that are currently supported are ARP caches, route tables, FIB tables, server tables, and interface tables. The number of valid entries in the table will be outputted at the end of the table display.

NOTE: The Network Tools connection to the device will be terminated upon execution of this command.

Syntax: **show <PROTOCOL> [TABLE]**

show mac <fid> [fdbId] <address> [mac] <port> [portNumber] <type> [<other | tp_learned | sr_learned |self | management>] [<priorityq |multicast | broadcast | staticfilt | agedout>]

show (Continued)

Options: **PROTOCOL** — Specifies a protocol for which information will be displayed.

TABLE — Specifies a type of table to display.

fid – Show MAC addresses for the filter database identifier (fdbId).

address – Show the address (mac) if it is known by the device.

port – Show the addresses for the port (portNumber) only.

type – Show addresses of the specified type only. Valid types are: other, tp_learned, sr_learned, self, management, priorityq, multicast, broadcast, staticfilt, agedout

Default – Show all MAC addresses for the device.

Examples:

```
-> show Appletalk interfaces

# Interface    AdminStatus    OperStatus      MTU      Forwarding    Framing
# 1            enabled        enabled         1500     enabled       ethernet
# 2            disabled       disabled        1500     disabled      ethernet
```

```
> show IP ARP

# Interface    MediaType      Physical|Address        NetworkAddress
#3             3(dynamic)     00:00:1d:04:40:5d       123.456.40.1
#4             3(dynamic)     08:00:20:0e:d8:31       123.456.40.30
# Number of valid entries: 2
```

```
-> show mac

MAC Address          FID          Port         Type

-----------------    ----------   ----------   ----------

00:00:1D:00:00:20             1   0010         tp_learned

00:00:1D:00:03:20             1   0010         tp_learned

00:00:1D:C3:BE:53             0   0001         self

00:00:1D:C3:BE:63             0   0017         self

more? (y or n)
```

soft_reset

Description: Restarts the software image, which restores the user configuration settings from NVRAM. The user will be queried to confirm the reset command to ensure against unwanted resets.

TIP: The Network Tools connection to the device will be terminated upon execution of this command.

Syntax: **soft_reset**

Options: None

Example:

```
->soft_reset

RESET: Are you *SURE* ?

-> Y
```

stpEdgePort

Description: Sets a port to EDGE PORT (enable) or BRIDGE PORT (disable).

Syntax:

stpEdgePort [status]

stpEdgePort [enable] [vlan id] [port range]

stpEdgePort [disable] [vlan id] [port range]

Options:

status — Displays STP edge port status.

enable — Enables one or more ports as STP edge ports.

disable — Disables one or more ports as STP edge ports.

vlan id — Specifies a VLAN ID.

port range — Specifies a range of ports.

Examples:

```
-> stpEdgePort enable 1 5

-> stpEdgePort enable 1 5-10
```

stpForceVersion

Description: Puts Spanning Tree into STP compatibility mode (0) or the default RSTP mode (2).

Syntax: **stpForceVersion [0 | 2 | status]**

Options: **stpForceVersion 0** – Indicates STP compatibility.

Enable stpForceVersion 0 only if the user does not want to “run 802.1w,” which does not allow transmission of RSTP BPDUs. The bridge will only transmit config BPDUs and TCNs. Therefore, to another bridge, it looks like it is running 802.1D (with few exceptions). This is only used if the potential of looping for 3 seconds (the time it takes a bridge to determine it is connected to a legacy device) could not be tolerated. The necessity of using this configuration is rare.

stpForceVersion 2 – Indicates RSTP support.

Status – Displays current value.

Example:

```
-> stpForceVersion 2
ForceVersion set to 2
```

stpLegacyPathCost

Description: Enables or disables the use of 802.1D or 802.1t Path Cost bridging values on the device. The default is legacy 802.1D standard Path Cost values.

NOTE: When connecting ports between devices, it is recommended that the devices are all set to run either 802.1D or 802.1t. The path costs must be consistent between bridge ports of all the devices.

Table 11-2 shows the path cost values when running 802.1t bridging.

Table 11-2 Path Cost Parameter Values

Link Speed	Recommended Value	Recommended Range	Range
10 Mb/s	2,000,000*	200,000-20,000,000	1-200,000,000
100 Mb/s	200,000*	20,000-2,000,000	1-200,000,000
1 Gb/s	20,000	2,000- 200,000	1-200,000,000
10 Gb/s	2,000	200-20,000	1-200,000,000

*Bridges conforming to IEEE Std 802.1D, 1998 Edition, i.e., that support only 16-bit values for Path Cost, must use 65,535 as the Path Cost for these link speeds when used in conjunction with Bridges that support IEEE Std 802.1t (32 bit) Path Cost values.

Syntax: **stpLegacyPathCost [enable | disable | status]**

Options: **enable** – Enables the device to use spanning tree legacy 802.1D Path Cost values.

disable – Returns the device to the default setting of using the spanning tree 802.1t Path Cost values.

status – Displays the current status of the Path Cost setting (enabled or disabled).

stpLegacyPathCost (Continued)

Examples:

To set the device to use the 802.1D legacy path costs, enter:

```
-> stpLegacyPathCost enable
```

To set the device to use the 802.1t path costs (default setting), enter:

```
-> stpLegacyPathCost disable
```

To determine if the device is currently operating using 802.1t or 802.1D path costs values, enter:

```
-> stpLegacyPathCost status
```

stpPointToPointMAC

Description: Displays the current values or sets the value of stpPointToPointMAC to TRUE, FALSE or AUTO.

Syntax:

stpPointToPointMAC [status] [value]

stpPointToPointMAC [value] [vlan id] [port range].

Options:

status — Displays the current stpPointToPointMAC settings.

value — Sets stpPointToPointMAC as true, false or auto, or displays settings with those values.

vlan id — Specifies a VLAN ID.

port range — Specifies a range of ports.

Examples:

Shows all VLAN ports with a value of true:

```
-> stpForceVersion MAC status true
```

Shows all VLAN ports with a value of false:

```
-> stpForceVersion MAC status false
```

Shows all VLAN ports with a value of auto:

```
-> stpForceVersion MAC status auto
```

Changes the value of stpForceVersion MAC for a port or range of ports.

```
-> stpForceVersion MAC auto 2 1-32
```

stpPort

Description: Enables, disables, or displays which physical ports are enabled as Spanning Tree ports. This command does not apply to virtual interfaces such as ATM. To enable, disable, or view the status of ATM ports, use the atm_stp_state command.

Syntax:

stpPort [status]

stpPort [enable] [port#]

stpPort [disable] [port#]

Options:

status — Displays a list of the physical ports that are enabled as Spanning Tree ports.

enable port# — Enables a specific port.

disable port# — Disables a specific port.

Examples:

```
-> stpPort status

The following ports are STP ENABLED:

1    2    3    4    5    6    7    8    9   10

11   12   13   14   15   16   17   18   19   20

21

-> stpPort enable 1
Enabling STP on Port 2.

-> stpPort disable 2

Disabling STP from Port 2.
```

stpRealTimeMsgAge

Description: Sets the BPDU MESSAGE AGE time mechanism to either IEEE or REAL TIME.

Syntax: **stpRealTimeMsgAge [enable | disable | status]**

Options:

enable – Enables the BPDU MESSAGE AGE time mechanism.

disable – Disables BPDU MESSAGE AGE time mechanism.

status – Displays the status of the BPDU MESSAGE AGE time mechanism.

stpRealTimeMsgAge (Continued)

Example:

```
stpRealTimeMsgAge disable
disabled
```

suppress_topology_traps

Description: Enables or disables the generation of topology traps on inter switch links. Only inter switch link ports that transition to forwarding or blocking cause the switch to issue a topology trap. By default, this feature is disabled and will allow the generation of topology traps.

Syntax: **suppress_topology_traps [enable | disable]**

Options: **enable** – Suppresses the generation of topology traps.

disable – Allows the generation of topology traps.

Example:

```
-> suppress_topology_traps enable
-> suppress_topology_traps disable
```

telnet

Description: Allows the user to communicate with another host (that supports Telnet connections) using the Telnet protocol. The user must specify the remote host using its IP address. The [IP address] field is mandatory. If no Port number is specified, telnet will attempt to contact the host at the default port.

Syntax: **telnet [IP address] <Port #>**

Options: **IP address** — Specifies the IP address of the host.

Port # — Specifies a Telnet port.

Example:

```
-> telnet 134.141.12.345
Trying 134.141.12.345
Connected to 134.141.12.345
SunOS UNIX (server 1)
login:
```

timed_soft_reset

Description: Configures a soft reset in number of seconds, or displays when a soft reset will occur. The reset_nv and dont_reset_nv commands tell the timed reset if non-volatile memory should be reset or not. If reset non_volatile is chosen, ip will be retained. Entering a time of 0 will disable any currently enabled timed_reset.

Syntax: **timed_soft_reset [status] [t (seconds)] [reset_nv | dont_reset_nv]**

Options: **status** — Displays the current timed soft reset setting.

t (seconds) — Specifies the number of seconds until the device will undergo a soft reset.

reset_nv — Resets non-volatile memory.

dont_reset_nv — Does not reset non-volatile memory.

Example:

```
-> timed_soft_reset status

timed_soft_reset 10

timed_soft_reset 30

timed_soft_reset 60 reset_nv
```

timed_reset

Description: Configures a timed reset in number of seconds, or displays when a reset will occur. The reset_nv and dont_reset_nv commands tell the timed reset if non-volatile memory should be reset or not. If reset non_volatile is chosen, ip will be retained. Entering a time of 0 will disable any currently enabled timed_reset.

Syntax: **timed_reset [status] [t (seconds)] [reset_nv | dont_reset_nv]**

timed_reset (Continued)

Options:

status — Displays the current timed reset setting.

t (seconds) — Specifies the number of seconds until the device will be reset.

reset_nv — Resets non-volatile memory.

dont_reset_nv — Does not reset non-volatile memory.

Examples:

```
-> timed_reset status

timed_reset 10

-> timed_reset 30

-> timed_reset 60 reset_nv
```

traceroute

Description: Generates a TRACEROUTE request to a specified IP address and provides a display of all next-hop routers in the path to the device. If the device is not reached, the command displays all next-hop routers to the point of failure.

Syntax: **traceroute [IP address]**

Options: **IP address** — Specifies the IP address of a device to which the traceroute will be generated.

Example:

```
-> traceroute 122.144.11.52

# next-hop[0]:122.144.60.45
# next-hop[1]:122.144.8.113
# next-hop[2]:122.144.61.45
# 122.144.11.52 is alive:3 hops away.
```

vrrpPort

Description: Enables, disables, or displays the status of Virtual Router Redundancy Protocol (VRRP) on front panel Ethernet or Fast Ethernet ports.

When the link on a VRRP Port goes down or up, the database is purged. Then a notification is sent out to all LAN emulation clients (LECs) connected to the local HSIM/VHSIM to clear their LEARP cache. Clearing the databases causes the removal of old information and forces the SmartSwitch devices to establish new virtual connections based on the new router paths.

NOTE: This command is only valid when the switch supports the installed HSIM or VHSIM.

Syntax:

vrrpPort [get]

vrrpPort [set] [port#]

vrrpPort [unset] [port#]

vrrpPort [set] [all]

vrrpPort [unset] [all]

Options:

get – Displays a list of all port numbers of VRRP Ports currently set.

set port# – Sets a specific port as a VRRP Port.

set all – Sets all front panel as VRRP Ports.

unset port# – Terminates the VRRP setting on a specific port.

unset all – Terminates the VRRP setting on all front panel ports.

NOTE: Setting the VRRP Port(s) to 0 will disable this application.

Examples:

```
-> vrrpPort get
VRRP Port is set to 0.

-> vrrpPort set 1
VRRP Port is set to 1.
```

11.3 EXAMPLE, EFFECTS OF AGING TIME ON DYNAMIC EGRESS

This section provides an example of how aging time affects the dynamic recognition of frames from a user device on a port.

In this example, assume that a rule set on Port 1 of the switch module classifies all IP frames to a Red VLAN. Once Port 1 receives a frame from a user device, the frame is classified to the Red VLAN and added to the dynamic Port VLAN List of Port 1.

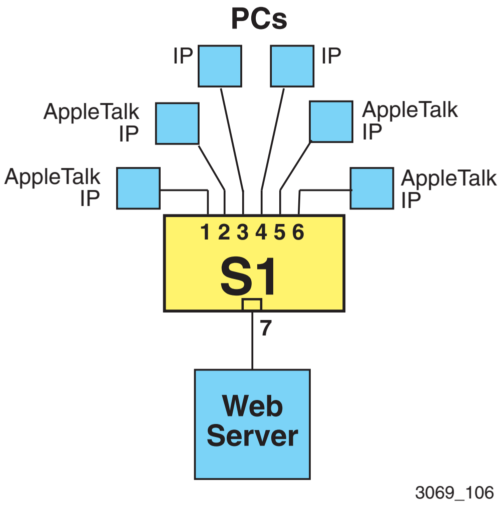
If after 300 seconds another IP frame is not received on Port 1 (by any station), the Red VLAN is removed from the dynamic Port VLAN List for Port 1. When Port 1 receives another frame, the Red VLAN is added again to the dynamic Port VLAN List of Port 1 and the process continues.

The dynamic Port VLAN List is a temporary list used in the dynamic egress function to keep track of the VLANs and the associated users that reside off a dynamic-egress enabled port.

11.4 EXAMPLE, USING DYNAMIC EGRESS TO CONTROL TRAFFIC

In this simple example (Figure 11-1), assume that there are four ports on the switch module attached to PCs supporting both protocols AppleTalk (809B and 80F3) and IP. Two PCs support IP only. The AppleTalk frame traffic is to be contained so only the users running the AppleTalk protocol can communicate with each other and not flood the network with AppleTalk frames. However, all users are to have access to a web server connected to Port 7.

Figure 11-1 Example, Dynamic Egress Application



Solving the Problem

In this example, Switch 1 (S1) has already been configured with a default VLAN 0001 associated with Filter Database Identifier (FDB ID) 0001 as the Port VLAN Identifier (PVID) on all ports.

The following additional steps are required to configure the switch to solve this problem.

1. Define a new VLAN (VLAN ID 2) using the Static VLAN Configuration screen.
2. Create a Layer 2 rule to associate the protocol AppleTalk 809B and 80F3 to VLAN ID 2 (VID 2) using the VLAN Classification Configuration screen. This rule is assigned to all ports.
3. Enable the dynamic egress control on VLAN 2 using the Network Tools command (**dynamic_egress enable 2**).

With the above configuration, an AppleTalk frame received on any port will be classified into VLAN 2 (the AppleTalk VLAN), and the Port VLAN List of that port is updated to include VLAN 2.

For instance, if Port 1 or 2 is connected to a new AppleTalk user, the AppleTalk frames received on that port are dynamically associated with VLAN 2 and VLAN 2 is added to the Port VLAN List of that port. The Port VLAN List contains a list of all VLANs whose frames can be transmitted out that port.

In this example, the AppleTalk traffic is routed only to AppleTalk users (Ports 1, 2, 5, and 6), while IP traffic is allowed to be seen by IP users (Ports 3, 4, and 7) and by IP/AppleTalk users (Ports 1, 2, 5, and 6).

11.5 SPECIAL COMMANDS

done, quit, exit	
Description:	The **done**, **quit**, or **exit** command enables the user to exit from Network Tools and return to the Main Menu screen.
Syntax:	done, quit, or exit
Options:	None

Example:	`-> ` **`done`**
	`Connection closed`

12

VLAN Operation and Network Applications

NOTE: It is recommended to read this chapter to gain an understanding of VLANs before configuring the switch.

This chapter provides the following information:

- Definition of VLANs (Section 12.1)
- Types of VLANs (Section 12.2)
- Benefits and Restrictions (Section 12.3) of VLANs
- VLAN Terms (Section 12.4)
- VLAN Operation (Section 12.5)
- Configuration Process (Section 12.6)
- VLAN Switch Operation (Section 12.7)
- VLAN Configuration (Section 12.8)
- Summary of VLAN Local Management (Section 12.9)
- Quick VLAN Walkthrough (Section 12.10) setting up a Static VLAN using Local Management
- Examples (Section 12.11) showing how VLAN-aware switches can be configured based on a given problem

12.1 DEFINING VLANs

A Virtual Local Area Network is a group of devices that function as a single Local Area Network segment (broadcast domain). The devices that make up a particular VLAN may be widely separated, both by geography and location in the network.

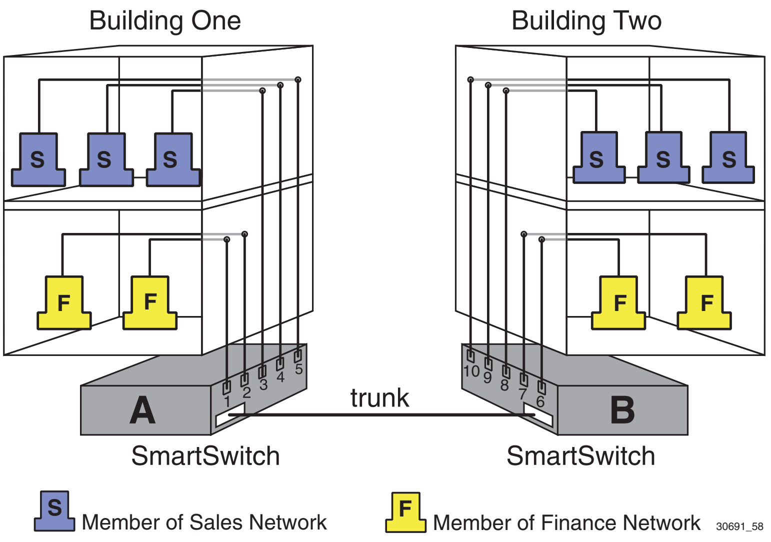
The creation of VLANs allows users located in separate areas or connected to separate ports to belong to a single VLAN group. Users that are assigned to such a group will send and receive broadcast and multicast traffic as though they were all connected to a common network.

VLAN-aware switches isolate broadcast, multicast, and unknown traffic received from VLAN groups, so that traffic from stations in a VLAN are confined to that VLAN.

When stations are assigned to a VLAN, the performance of their network connection is not changed. Stations connected to switched ports do not sacrifice the performance of the dedicated switched link to participate in the VLAN. As a VLAN is not a physical location, but a membership, the network switches determine VLAN membership by associating a VLAN with a particular port or frame type.

Figure 12-1 shows a simple example of a port-based VLAN. Two buildings house the Sales and Finance departments of a single company, and each building has its own internal network. The stations in each building connect to a SmartSwitch in the basement. The two SmartSwitches are connected to one another with a high speed link.

Figure 12-1 Example of a VLAN



In this example, the Sales and Finance workstations have been placed on two separate VLANs. In a plain Ethernet environment, the entire network is a broadcast domain, and the SmartSwitches follow the IEEE 802.1D bridging specification to send data between stations. A broadcast or multicast transmission from a Sales workstation in Building One would propagate to all the switch ports on SmartSwitch A, cross the high speed link to SmartSwitch B, and then propagated out all switch ports on SmartSwitch B. The SmartSwitches treat each port as being equivalent to any other port, and have no understanding of the departmental memberships of each workstation.

In a VLAN environment, each SmartSwitch understands that certain individual ports or frames are members of separate workgroups. In this environment, a broadcast or multicast data transmission from one of the Sales stations in Building One would reach SmartSwitch A, be sent to the ports connected to other local members of the Sales VLAN, cross the high speed link to SmartSwitch B, and then be sent to any other ports and workstations on SmartSwitch B that are members of the Sales VLAN.

12.2 TYPES OF VLANs

There are a number of different strategies for creating Virtual Local Area Networks, each with their own approaches to defining a station’s membership in a particular VLAN.

12.2.1 802.1Q VLANs

An 802.1Q VLAN switch determines the VLAN membership of a data frame by its Tag Header, described later in this chapter. If the frame received is not tagged, the switch classifies the frame into the VLAN that is assigned as the default VLAN of the switch.

Some or all ports on the switch may be configured to operate as GARP VLAN Registration Protocol (GVRP) ports. If a frame received is tagged, the frame is forwarded to the GVRP ports that are configured to transmit frames associated with the frame VLAN ID and protocol. If the received frame is not tagged, the frame is examined and tagged as belonging to the default VLAN. Then the frame is forwarded to the GVRP ports that are configured to transmit frames associated with the default VLAN and the frame protocol.

12.2.2 Other VLAN Strategies

VLANs may also be created by a variety of addressing schemes, including the recognition of groups of MAC addresses or types of traffic. One of the best-known VLAN-like schemes is the use of IP Subnets to divide networks into smaller subnetworks.

12.3 BENEFITS AND RESTRICTIONS

The primary benefit of the 802.1Q VLAN technology is that it provides localization of traffic. This function also offers improvements in security and performance to stations assigned to a VLAN.

While the localization of traffic to VLANs can improve security and performance, it imposes some restrictions on network devices that participate in the VLAN. Through the use of Filtering Database IDs (FDB IDs) security can be implemented to enable or prevent users from one or more VLANs from communicating with each other.

One or more VLANs can be assigned to an FDB ID so that all the users that share a common FDB ID can communicate with each other regardless of their VLAN affiliation. However, for the sake of security, the members of one FDB ID cannot communicate with the members of another FDB ID.

To set up a VLAN, all the network switch devices that are assigned to the VLAN must support the IEEE 802.1Q specification for VLANs. Before you attempt to implement a VLAN strategy, ensure that the switches under consideration support the IEEE 802.1Q specification.

12.4 VLAN TERMS

To fully understand the operation and configuration of port based VLANs, it is essential to understand the definitions of several key terms.

Table 12-1 VLAN Terms and Definitions

VLAN Term	Definition
VLAN ID	A unique number (between 1 and 4094) that identifies a particular VLAN. Up to 1000 VLANs can be created on one SmartSwitch.
VLAN Name	A 32-character alphanumeric name associated with a VLAN ID. The VLAN Name is intended to make user-defined VLANs easier to identify and remember.
Egress	Output direction of data from a network device.
Ingress	Incoming direction of data to a network device.

Table 12-1 VLAN Terms and Definitions (Continued)

VLAN Term	Definition
Filtering Database Identifier (FDB ID)	Addressing information that the device learns about a VLAN is stored in the filtering database assigned to that VLAN. Several VLANs can be assigned to the same FDB ID to allow those VLANs to share addressing information. This enables the devices in the different VLANs to communicate with each other when the individual ports have been configured to allow communication to occur. The configuration is accomplished using the Local Management VLAN Forwarding Configuration screen. By default a VLAN is assigned to the FDB ID that matches its VLAN ID.
Tag Header (VLAN Tag)	Four bytes of data inserted in a frame that identifies the VLAN/frame classification. The Tag Header is inserted into the frame directly after the Source MAC address field. Twelve bits of the Tag Header represent the VLAN ID. The remaining bits are other control information.
Tagged Frame	A data frame that contains a Tag Header. A VLAN-aware device can add the Tag Header to any frame it transmits.
Untagged Frame	A data frame that does not have a Tag Header.
Default VLAN	The VLAN to which all ports are assigned upon initialization. The Default VLAN has a VLAN ID of 1 and cannot be deleted or renamed.
Forwarding List	A list of the ports on a particular device that are eligible to transmit frames for a selected VLAN.
Port VLAN List	A per port list of all eligible VLANs whose frames can be forwarded out one specific port and the frame format (tagged or untagged) of transmissions for that port. The Port VLAN List specifies what VLANs are associated with a single port for frame transmission purposes.
Filtering Database	A database structure within the switch that keeps track of the associations between MAC addresses, VLANs, and interface (port) numbers. The Filtering Database is referred to when a switch makes a forwarding decision on a frame.

Table 12-1 VLAN Terms and Definitions (Continued)

VLAN Term	Definition
1Q Connection (previously referred to as a 1Q Trunk)	A connection between 802.1Q switches that passes only traffic with a VLAN Tag Header inserted in each frame. All VLANs in the port's Port VLAN List are configured to transmit all frames as tagged frames. The port will drop all incoming frames that do not have a VLAN tag.
1D Connection	This is a reference to a connection from a switch that passes only untagged traffic. By default, a port designated to pass only untagged frames has all VLANs on its Port VLAN List and is configured to transmit all frames as untagged frames. **NOTE:** You cannot configure an interface to receive only untagged frames.
Per VLAN Spanning Tree Protocol (PVSTP)	A protocol used to create a separate Spanning Tree topology for each VLAN configured in a switch.
Quick Convergence STP (QCSTP)	A protocol that is compatible with PVSTP and provides automatic topology changes at 1/10th the speed of PVSTP. QCSTP is also backwards compatible with IEEE 802.1D.
Generic Attribute Registration Protocol (GARP)	A protocol used to propagate state information throughout a switched network.
GARP VLAN Registration Protocol (GVRP)	A GARP application used to dynamically create VLANs across a switched network.
GARP Multicast Registration Protocol (GMRP)	A GARP application that functions in a similar fashion as GVRP, except that GMRP registers multicast addresses on ports to control the flooding of multicast frames. **NOTE:** GMRP is not supported in this device.

12.5 VLAN OPERATION

The following sections describe the operation of a VLAN switch and discusses the operations that a VLAN switch performs in response to both normal and VLAN-originated network traffic.

12.5.1 Description

The 802.1Q VLAN operation is slightly different than the operation of traditional switched networking systems. These differences are due to the importance of keeping track of each frame and its VLAN association as it passes from switch to switch or from port to port within a switch.

12.5.2 VLAN Components

Before describing the operation of an 802.1Q VLAN, it is important to understand the basic elements that are combined to make up an 802.1Q VLAN.

Stations

A station is any end unit that belongs to a network. In the vast majority of cases, stations are the computers through which the users access the network.

Switches

In order to configure a group of stations into a VLAN, the stations must be connected to VLAN-aware switches. It is the job of the switch to classify received frames into VLAN memberships and transmit frames, according to VLAN membership, with or without a VLAN Tag Header.

12.6 CONFIGURATION PROCESS

Before a VLAN can operate, steps must be performed to configure the switch to establish and configure a VLAN. Enterasys Networks VLAN-aware SmartSwitches default to operate in the 802.1Q VLAN mode. However, further configuration is necessary to establish multiple logical networks.

NOTE: The actual steps involved in VLAN configuration using Local Management are presented in Section 12.8. This brief section describes the actions that must be taken in very general terms, and is intended only to aid in the Administrator’s understanding of VLAN switch operation.

12.6.1 Defining a VLAN

A VLAN must exist and have a unique identity before any ports or rules can be assigned to it. The Administrator defines a VLAN by assigning it a unique identification number (the VLAN ID), a filter database association, and an optional name. The VLAN ID is the number that will identify data frames originating from, and intended for, the ports that will belong to this new VLAN.

12.6.2 Classifying Frames to a VLAN

Now that a VLAN has been created, rules are defined to classify all frames in a VLAN. This is accomplished through management by associating a VLAN ID with each port on the switch. Optionally, frames can be classified according to layer 2/3/4 information contained in the frame.

At the same time, the Administrator configures the trunk ports that need to consider themselves members of every VLAN. The configuration of trunk ports is very important in multiswitch VLAN configurations where a frame's VLAN membership needs to be maintained across several switches.

12.6.3 Customizing the VLAN Forwarding List

Each port on a VLAN-aware switch has a VLAN forwarding list that contains, as a minimum, the Port VLAN Identifier (PVID) of the VLAN configured. Additionally, the Port VLAN Forwarding List of each port can be configured to allow any number of VLANs to be added to its list.

12.7 VLAN SWITCH OPERATION

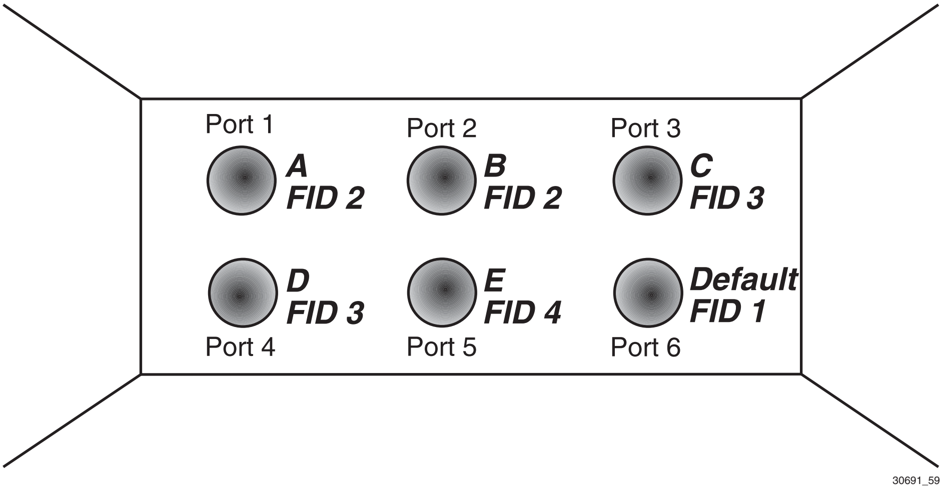
IEEE 802.1Q VLAN switches act on the classification of frames into VLANs. Sometimes, VLAN classification is based on tags in the headers of data frames. These VLAN tags are added to data frames by the switch as the frames are transmitted out certain ports, and are later used to make forwarding decisions by the switch and other VLAN-aware switches.

In the absence of a VLAN tag header, the classification of a frame into a particular VLAN depends upon the configuration of the switch port that received the frame.

The operation of an 802.1Q VLAN switch is best understood from a point of view *of* the switch itself. To illustrate this concept, the examples that follow view the switch operations from *inside* the switch.

Figure 12-2 depicts the inside of a switch with six ports, numbered one through six. The switch has been configured to associate VLAN A and B with Filtering Database Identifier (FDB ID) 2, VLAN C and D with FDB ID 3, and VLAN E with FDB ID 4. Port 6 has been classified to serve as a VLAN trunk connection (will only transmit and receive tagged frames). This classification establishes that all VLANs are members of the Port VLAN List for Port 6 and the frames transmitted for all VLANs will contain a tag header. Also the PVID for Port 6 is set to the default VLAN with its corresponding relationship to FDB ID 1. Although untagged frames are not usually present on a VLAN trunk connection, any untagged frames received would need to be classified if the port has not been configured to drop all untagged frames.

Figure 12-2 View from Inside the Switch



NOTE: The example in Figure 12-2 shows ports sharing the same FDB ID, which is supported by the switch. However, this feature cannot be configured using Local Management at this time, but it can be configured using an SNMP management application.

12.7.1 Receiving Frames from VLAN Ports

When a switch is placed in 802.1Q Operational Mode, every frame received by the switch must belong, or be assigned, to a VLAN.

Untagged Frames

The switch receives a frame from Port 1 and examines the frame. The switch notices that this frame does not currently have a VLAN tag. The switch recognizes that Port 1 is a member of VLAN A and classifies the frame as such. In this fashion, all untagged frames entering a VLAN switch assume membership in a VLAN.

NOTE: A VLAN ID is always assigned to a port. By default, it is the Default VLAN (VLAN ID = 1).

The switch will now make a forwarding decision on the frame, as described in Section 12.7.2.

Tagged Frames

In this example, the switch receives a tagged frame from Port 4. The switch examines the frame and notices the frame is tagged for VLAN C. This frame may have already been through a VLAN-aware switch, or originated from a station capable of specifying a VLAN membership. If a switch receives a frame containing a tag, the switch will classify the frame in regard to its tag rather than the PVID for its port.

The switch will now make a forwarding decision on the frame, as described in Section 12.7.2.

12.7.2 Forwarding Decisions

The type of frame under consideration and the filter setting of a VLAN switch determines how the switch forwards VLAN frames.

12.7.2.1 Broadcasts, Multicasts, and Unknown Unicasts

If a frame with a broadcast, multicast, or other unknown address is received by an 802.1Q VLAN-aware switch, the switch checks the VLAN classification of the frame. The switch then forwards the frame out all ports that are identified in the Egress List for that VLAN. For example, if Port 3, shown in Figure 12-2, received the frame, the frame would then be sent to all ports that had VLAN C in their Port VLAN List.

12.7.2.2 Known Unicasts

When a VLAN switch receives a frame with a known MAC address as its destination address, the action taken by the switch to determine how the frame is transmitted depends on the VLAN, the VLAN associated FDB ID, and if the port identified to send the frame is enabled to do so.

When a frame is received it is classified into a VLAN. The destination address is looked up in the FDB ID associated with the VLAN. If a match is found, it is forwarded out the port identified in the lookup if, and only if, that port is allowed to transmit frames for that VLAN. If a match is not found, then the frame is flooded out all ports that are allowed to transmit frames belonging to that VLAN.

For example, assume that a frame is received by the switch depicted back in Figure 12-2. This frame is a unicast untagged frame received on Port 3. The frame is then classified for VLAN C. The switch then makes its forwarding decision by comparing the destination MAC address to its filtering database. In this case, the MAC address is looked up in the filtering database FDB ID 3, which is associated with VLAN C and VLAN D. The switch recognizes the destination MAC address of the frame as being located out Port 4.

Having made the forwarding decision, the switch now examines the Port VLAN List of Port 4 to determine if it may transmit a frame belonging to VLAN C. If so, the frame is transmitted out Port 4. If Port 4 has not been configured to transmit frames belonging to VLAN C, the frame is discarded.

12.8 VLAN CONFIGURATION

This section describes how to set up the switch for local or remote management, and the VLAN Local Management screens used to create and configure VLANs in a SmartSwitch.

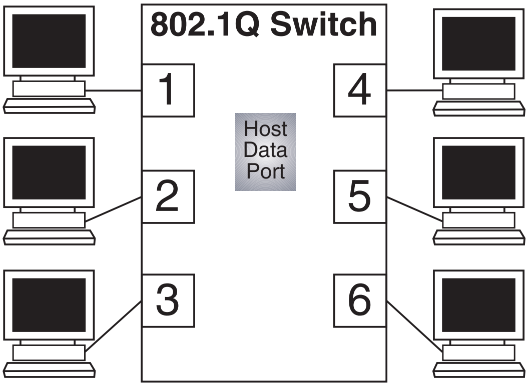
12.8.1 Managing the Switch

The switch may be managed locally via a terminal connected to the COM port, or remotely (SNMP or Telnet sessions) from a management station connected to a switch port that is a member of the same VLAN as the switch’s Host Data Port. (By default, this is the default VLAN.) When the switch is configured with VLANs, special precautions must be taken to use remote management.

12.8.2 Switch Without VLANs

When the switch is powered up, the switch uses its default settings to switch frames like an 802.1Q switch. In this default configuration, all ports are a member of the default VLAN (VLAN 1) including the virtual Host Data Port of the switch, so any port can be used to manage the device as shown in Figure 12-3.

Figure 12-3 Switch Management with Only Default VLAN



NOTE: All ports, including the virtual Host Data Port, are members of the default VLAN. Therefore, any station shown may be used as the management station.

30691_60

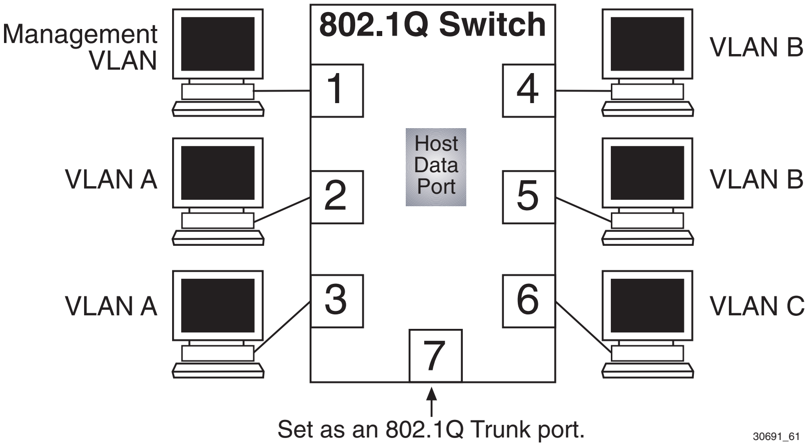
12.8.3 Switch with VLANs

If the switch is to be configured for multiple VLANs, it may be desirable to configure a management-only VLAN. This allows a management station connected to the management VLAN to manage all ports on the switch and make management secure by preventing management via ports assigned to other VLANs.

NOTE: The switch's virtual Host Data Port, like any other port, has VLAN membership that is configurable. For manageability of the device to be maintained, this port must be a member of the same VLAN as the port to which the management station is connected.

Figure 12-4 shows an example of a switch configured with port 1 on the Management VLAN port and the other users belonging to VLANs A, B, and C.

Figure 12-4 Switch Management with VLANs



To set up the switch shown in Figure 12-4 to establish a management VLAN on port 1, use the following process:

1. Use the Static VLAN Configuration screen to define a new VLAN named “Management VLAN” (or other suitable name) and its VLAN ID. In this example, the VLAN ID is set to 2.

   An FDB ID is automatically assigned by the switch, so that the Management VLAN has its filtering database to make the VLAN secure. In this example, the FDB ID is 2 and no other VLAN is assigned to this FDB ID. This keeps the new VLAN from sharing its filtering database with other VLANs in the switch.

2. Use the Static VLAN Egress Configuration screen to associate the ports to particular VLANs. For details on defining a Static VLAN, refer to Section 7.3.1.

3. Use the Static VLAN Egress Configuration screen to select the type of Egress setting for each port. When a port is set as Tagged, a VLAN tag is inserted into each frame transmitted out the port to associate it with the VLAN specified at the top of the screen.

4. Use the VLAN Port Configuration screen to enter the VLAN ID, 2, of the new Management VLAN as the Port VLAN ID (PVID) to a port. In this example, it is port 1. Leave the Acceptable Frame Types setting in the default value, ADMIT ALL FRAMES.

NOTE: It is not necessary to configure a physical port for management on each switch. Only those switches that will have a management station attached to it need a physical port assigned to the Management VLAN.

5. Use the VLAN Port Configuration screen to enter the VLAN ID, 2, of the new Management VLAN as the Port VLAN ID (PVID) to the Host Data Port. The port number will depend on the device. This port is not a physical port and will usually be one number above the maximum number of physical ports on the device, including the ports on any optional interfaces installed. In this example, it will be port 8. Set the Acceptable Frame Types setting to the setting: ADMIT VLAN ALL FRAMES. For details on assigning a PVID, refer to Section 7.7.

This process would be repeated on every switch that is connected in the network to ensure that each switch has a secure Management VLAN for switch management.

If the switch was connected to another switch via port 7, which was set to pass only tagged frames, then the management station connected to the Management VLAN port of either switch could manage both switches

NOTE: The management stations at each switch must be on the same Management VLAN.

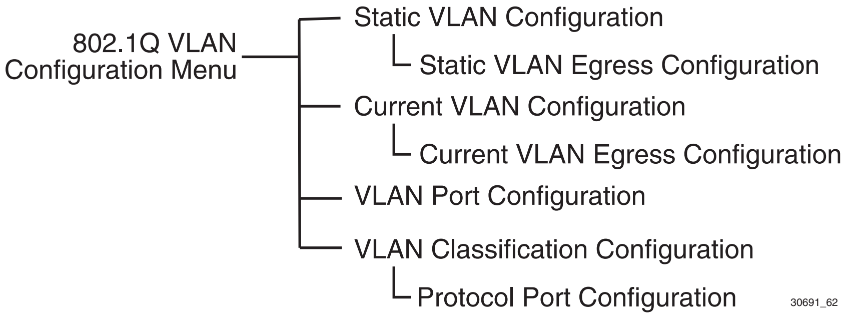
No matter how many switches are connected, a management station connected to any port on the same Management VLAN can be used to remotely manage any Enterasys Networks 802.1Q switch in the network as long as the Host Data Port of all the switches are members of the same Management VLAN.

12.9 SUMMARY OF VLAN LOCAL MANAGEMENT

The VLAN configuration process is an extension of normal Local Management operations. A series of Local Management screens provides access to the functions and commands necessary to add, change, or delete VLANs and to assign ports to those VLANs.

A switch supporting 802.1Q VLANs provides the VLAN Configuration screens as a standard part of its Local Management hierarchy when the switch is configured to operate in 802.1Q Mode. The hierarchy of the Local Management screens pertaining to 802.1Q VLAN configuration is shown in Figure 12-5.

Figure 12-5 802.1Q VLAN Screen Hierarchy


802.1Q VLAN Configuration Menu
Static VLAN Configuration
Static VLAN Egress Configuration
Current VLAN Configuration
Current VLAN Egress Configuration
VLAN Port Configuration
VLAN Classification Configuration
Protocol Port Configuration
30691_62

For details about each screen and how to use them, refer to Chapter 7.

12.9.1 Preparing for VLAN Configuration

A little forethought and planning is essential to a good VLAN implementation. Before attempting to configure a single switch for VLAN operation, consider the following:

- How many VLANs will be required?
- What stations will belong to them?
- What ports are connected to those stations?
- What ports will be configured as GARP-aware ports?
- Will Per VLAN Spanning Tree or Quick Convergence Spanning Tree be used?

It may also be helpful to sketch out a diagram of your VLAN strategy. The examples provided starting with Section 12.11 may be useful for a depiction of the planning process. Section 12.10 provides a quick walkthrough on how to use the screens to configure the switch for VLANs.

12.10 QUICK VLAN WALKTHROUGH

The procedures below provide a short tutorial walkthrough that presents each of the steps necessary to configure a new Static VLAN. These steps include the following:

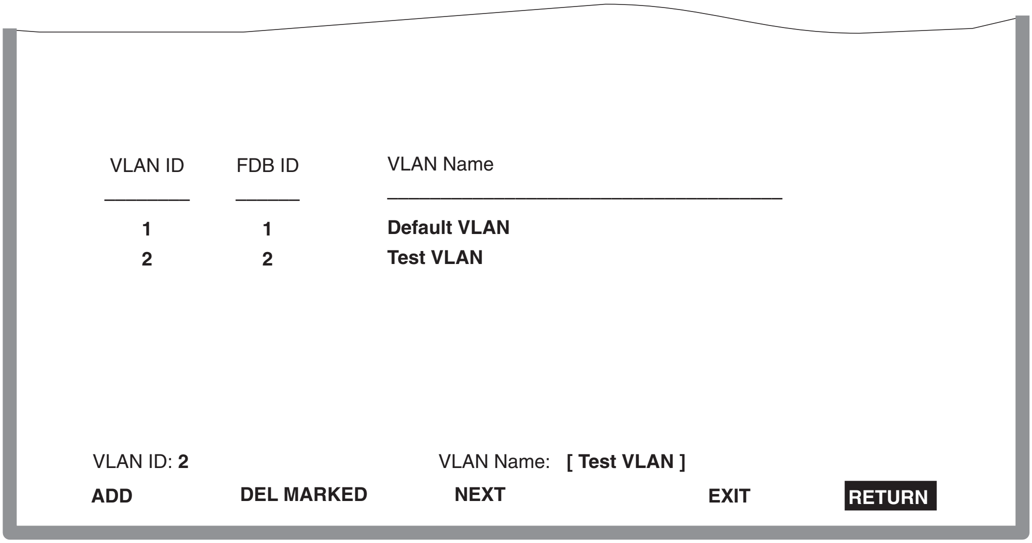
- Assigning a VLAN ID and VLAN Name
- Assigning ports to the VLAN Egress list
- Configuring the port parameters

You may want to follow this walkthrough from start to finish before attempting to configure your own VLANs. This walkthrough begins at the 802.1Q VLAN Configuration Menu screen.

Assigning a VLAN ID and VLAN Name

1. On the 802.1Q VLAN Configuration Menu screen, use the arrow keys to highlight the **STATIC VLAN CONFIGURATION** menu item. Press ENTER. The Static VLAN Configuration screen displays.
2. On the Static VLAN Configuration screen, use the arrow keys to highlight the **VLAN ID** field at the bottom of the screen. Assign a number for a new VLAN by typing the number “**2**” in the **VLAN ID** field. A Filtering Database Identified (FDB ID) will automatically be assigned to the VLAN ID.
3. Use the arrow keys to highlight the **VLAN Name** field at the bottom of the screen. Type “**TEST VLAN**” in the VLAN Name field. Press ENTER.
4. Use the arrow keys to highlight the **ADD** command field at the bottom of the screen. Press ENTER. The new VLAN is created and added to the list in the screen as shown in Figure 12-6.

Figure 12-6 Walkthrough Stage One, Static VLAN Configuration Screen



```
  VLAN ID      FDB ID        VLAN Name
  -------      ------        --------------------------------
     1            1          Default VLAN
     2            2          Test VLAN




VLAN ID: 2                          VLAN Name:  [ Test VLAN ]
ADD          DEL MARKED          NEXT              EXIT         RETURN
```

Assigning Ports to the VLAN Egress list

1. Use the arrow keys to highlight the line in the list that has VLAN ID 2. As shown in Figure 12-6, the Static VLAN Egress Configuration screen displays showing all ports.
   It is now time to assign a port to this new VLAN.

NOTE: When a Static VLAN is created, all ports on the Static VLAN Egress Configuration screen are set to the default setting of NO for that VLAN. This means that none of the ports are on the Egress list for that VLAN and will not transmit its frames.

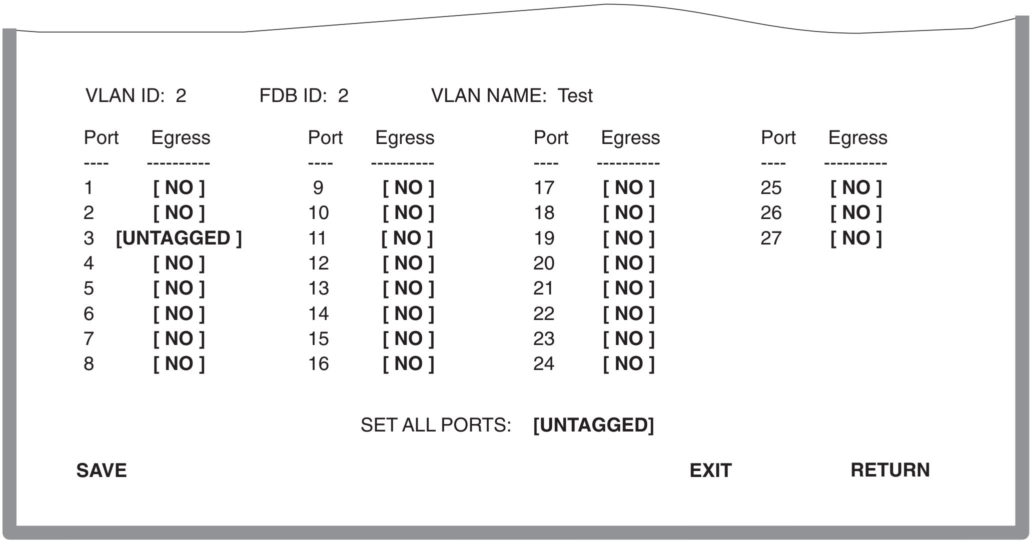
2. Use the arrow keys to highlight the **Egress** field of Port 3.

NOTE: For the purposes of this walkthrough, Port 3 will be configured. As this port will connect to a single workstation, and is not to be used for switch-to-switch communications, the Egress will be set to UNTAGGED.

3. Use the SPACE bar to step to **UNTAGGED**.

4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen. Press ENTER. Port 3 is added to the Egress list of VLAN 2 with a frame format of UNTAGGED. The screen should now look like Figure 12-7.

Figure 12-7 Walkthrough Stage Two, Port 3 Egress Setting



```
     VLAN ID:  2          FDB ID:  2          VLAN NAME:  Test

     Port     Egress            Port     Egress            Port     Egress            Port     Egress
     ----     ----------        ----     ----------        ----     ----------        ----     ----------
     1         [ NO ]            9        [ NO ]           17        [ NO ]           25        [ NO ]
     2         [ NO ]           10        [ NO ]           18        [ NO ]           26        [ NO ]
     3    [UNTAGGED ]           11        [ NO ]           19        [ NO ]           27        [ NO ]
     4         [ NO ]           12        [ NO ]           20        [ NO ]
     5         [ NO ]           13        [ NO ]           21        [ NO ]
     6         [ NO ]           14        [ NO ]           22        [ NO ]
     7         [ NO ]           15        [ NO ]           23        [ NO ]
     8         [ NO ]           16        [ NO ]           24        [ NO ]

                                  SET ALL PORTS:   [UNTAGGED]

    SAVE                                                        EXIT            RETURN
```

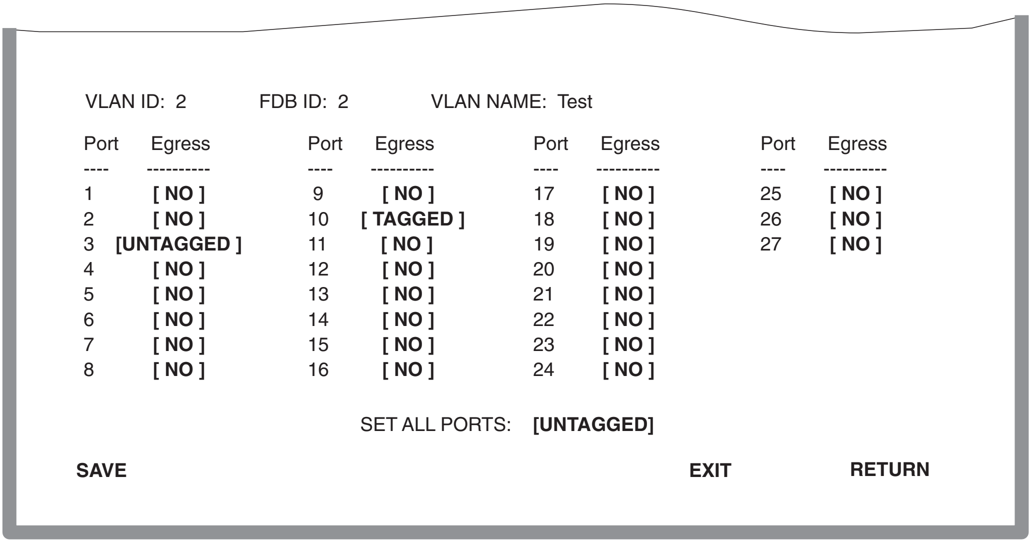
30691_64

Now that Port 3 belongs to VLAN 2, we will designate one port as a trunk port for a connection to another VLAN-aware switch. This trunk port will carry tagged frames from all VLANs, allowing VLAN frames to maintain their VLAN ID across multiple switches.

NOTE: For the purposes of this walkthrough, port 10 will be configured as the trunk port.

5. Use the arrow keys to highlight the **Egress** field for port 10 in the Static VLAN Egress Configuration screen.
6. Use the SPACE bar to step to **TAGGED**.
7. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen. Press ENTER. Port 10 will now serve as a trunk port connection. The screen should now look like Figure 12-8.

Figure 12-8 Walkthrough Stage Three, Port 10 Egress Setting



```
VLAN ID:  2          FDB ID:  2          VLAN NAME:  Test

Port     Egress            Port     Egress           Port     Egress           Port     Egress
----     ----------        ----     ----------       ----     ----------       ----     ----------
1          [ NO ]           9         [ NO ]         17       [ NO ]           25       [ NO ]
2          [ NO ]          10     [ TAGGED ]         18       [ NO ]           26       [ NO ]
3     [UNTAGGED ]          11         [ NO ]         19       [ NO ]           27       [ NO ]
4          [ NO ]          12         [ NO ]         20       [ NO ]
5          [ NO ]          13         [ NO ]         21       [ NO ]
6          [ NO ]          14         [ NO ]         22       [ NO ]
7          [ NO ]          15         [ NO ]         23       [ NO ]
8          [ NO ]          16         [ NO ]         24       [ NO ]

                         SET ALL PORTS:   [UNTAGGED]

SAVE                                                       EXIT          RETURN
```

30691_65

Configuring the Port Parameters

Now that the TEST VLAN and the trunk connection are set up, we can proceed to set the port parameters for ports 3 and 10, as follows:

1. On the 802.1Q Configuration Menu screen, use the arrow keys to highlight the **VLAN PORT CONFIGURATION** menu item and press ENTER. The VLAN Port Configuration screen, Figure 12-9, displays.
2. Use the arrow keys to highlight the **PVID** field for Port 3.
3. Type in **2**, which is the VLAN ID of the Test VLAN. This will associate Port 3 with the VLAN ID, thus making the port PVID of 2.

NOTE: Since Port 3 will connect to a single workstation, and is not to be used for switch-to-switch communications, the acceptable frame types allowed through this port will be all frame types (tagged and untagged). Since Port 3 will not receive VLAN frames from the work station, it is not necessary to filter frames.

4. Use the arrow keys to highlight the **Acceptable Frame Types** field for Port 3.
5. Use the SPACE bar to step to **ADMIT ALL FRAMES**.
6. Leave the **INGRESS FILTERING** field for Port 3 in the default setting of **DISABLED**. This prevents frames from being filtered out according to the Port VLAN List.

7. Leave the **GVRP STATUS** field for Port 3 in the default setting of **ENABLED**. This sets Port 10 as a GVRP port to receive registrations of dynamically created VLANs.

8. Leave the **PVID** field for Port 10 set in the default setting of 1.

NOTE: Since Port 10 will be used for switch-to-switch communications, the PVID is left set on the default VLAN value of 1. This associates Port 10 with all VLANs on the switch. Since Port 10 will be used as a trunk port, only tagged frames will be allowed through the port.

9. Use the arrow keys to highlight the **Acceptable Frame Types** field for Port 10.

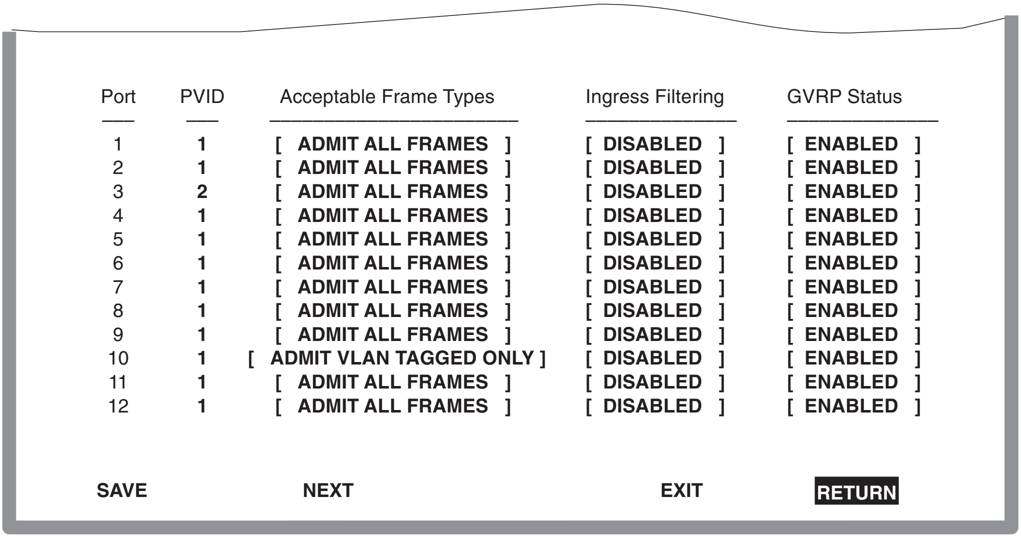
10. Use the SPACE bar to step to **ADMIT VLAN TAGGED ONLY**. This causes Port 10 to drop all frames received that are untagged.

11. Leave the **INGRESS FILTERING** field for Port 3 in the default setting of **DISABLED**.

12. Leave the **GVRP STATUS** field for Port 3 in the default setting of **ENABLED**. This sets Port 10 as a GVRP port to pass tagged frames of dynamically created VLANs.

13. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen. Press ENTER. The screen should now look like Figure 12-9.

Figure 12-9 Walkthrough Stage Four, VLAN Port Configuration



```
Port    PVID      Acceptable Frame Types        Ingress Filtering     GVRP Status
----    ----    --------------------------      ---------------      ---------------
 1       1      [  ADMIT ALL FRAMES   ]         [ DISABLED  ]        [ ENABLED  ]
 2       1      [  ADMIT ALL FRAMES   ]         [ DISABLED  ]        [ ENABLED  ]
 3       2      [  ADMIT ALL FRAMES   ]         [ DISABLED  ]        [ ENABLED  ]
 4       1      [  ADMIT ALL FRAMES   ]         [ DISABLED  ]        [ ENABLED  ]
 5       1      [  ADMIT ALL FRAMES   ]         [ DISABLED  ]        [ ENABLED  ]
 6       1      [  ADMIT ALL FRAMES   ]         [ DISABLED  ]        [ ENABLED  ]
 7       1      [  ADMIT ALL FRAMES   ]         [ DISABLED  ]        [ ENABLED  ]
 8       1      [  ADMIT ALL FRAMES   ]         [ DISABLED  ]        [ ENABLED  ]
 9       1      [  ADMIT ALL FRAMES   ]         [ DISABLED  ]        [ ENABLED  ]
10       1    [  ADMIT VLAN TAGGED ONLY ]       [ DISABLED  ]        [ ENABLED  ]
11       1      [  ADMIT ALL FRAMES   ]         [ DISABLED  ]        [ ENABLED  ]
12       1      [  ADMIT ALL FRAMES   ]         [ DISABLED  ]        [ ENABLED  ]


SAVE                NEXT                          EXIT             RETURN
```

This effectively completes the configuration of a single VLAN, assigning it to a port, and configuring the switch to forward the frames received on that port to a trunk port. The trunk port in turn forwards the frames as tagged to another switch.

You can now use the VLAN Classification Configuration and Port Protocol Configuration screens to transmit frames according to classification rules and associated ports, as described in Chapter 7.

12.11 EXAMPLES

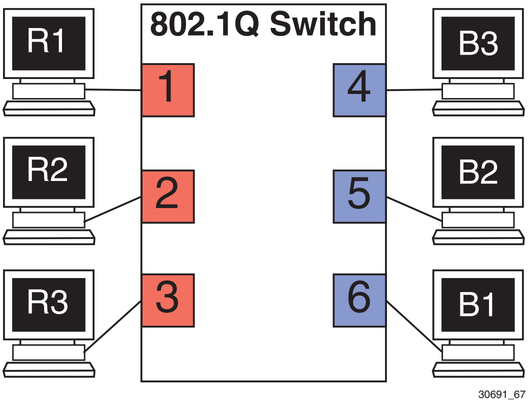
NOTE: Due to the complexity of Local Management, the following simple examples are not meant to cover the full potential of Local Management.

The following sections provide some examples of how VLAN-aware SmartSwitches can be configured to group users at the port level to create VLANs in existing networks. Each example presents a problem and shows how it is solved by configuring the switches using the VLAN Local Management screens. The actual procedures and screens used to configure a VLAN-aware switch are covered in Chapter 7. Also provided in the discussion of each example is a description of how the frames transmitted from one user would traverse the network to its target device.

12.12 EXAMPLE 1, SINGLE SWITCH OPERATION

This first example looks at the configuration of a single Ethernet switch for VLAN operation. In this example, two groups of three users are to be assigned to two VLANs to isolate them from one another. The blue users (B1, B2, B3) are to be kept completely separate from the red users (R1, R2, R3). Figure 12-10 shows the initial state of the switch.

Figure 12-10 Example 1, Single Switch Operation



12.12.1 Solving the Problem

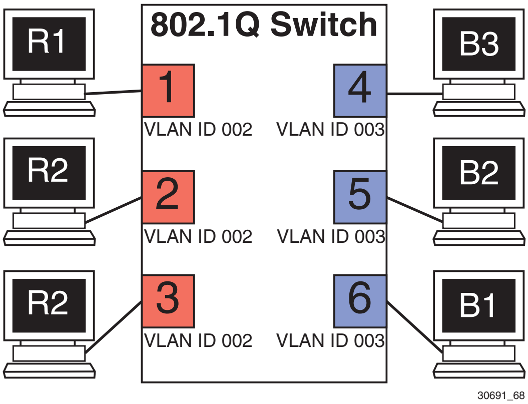
To set up this switch, users will be assigned to two new VLANs, red stations to the Red VLAN, and blue stations to the Blue VLAN. The information below describes how the switch is configured to create these two VLANs and how users are assigned to them.

1. The switch is set for 802.1Q operation.
2. VLAN ID 2 (Red VLAN) and VLAN ID 3 (Blue VLAN) are created using the Static VLAN Configuration screen. The filter database FDB ID 2 and FDB ID 3 are automatically assigned to the Red VLAN and Blue VLAN, respectively.
3. The Egress type for each port associated with a VLAN is set using the Static VLAN Egress Configuration screen. In this example, the settings are as follows:
   - For the Red VLAN
     Ports 1, 2, and 3; Egress; UNTAGGED
   - For the Blue VLAN
     Ports 4, 5, and 6; Egress; UNTAGGED
4. The ports 1 through 6 are configured as follows using the VLAN Port Configuration screen:
   - Ports 1, 2, and 3 are set as follows:

     PVID: 2
     Acceptable Frame Types: ADMIT ALL FRAMES
     Ingress Filtering: ENABLED
     GVRP Status: DISABLED
   - Ports 4, 5, and 6 are set as follows:

     PVID: 3
     Acceptable Frame Types: ADMIT ALL FRAMES
     Ingress Filtering: ENABLED
     GVRP Status: DISABLED
5. The VLANs and ports are now configured and enabled. Figure 12-11 shows the resulting VLAN assignment to each port.

Figure 12-11 Switch Configured for VLANs



The switch will now classify each frame received as belonging to either the Red or Blue VLANs. Traffic from one VLAN will not be forwarded to the members of the other VLAN, and all frames transmitted by the switch will be normal, untagged Ethernet frames.

12.12.2 Frame Handling

This section describes the operations of the switch when two frames are received. The first frame is a broadcast sent by station R1.

1. Station R1 transmits the broadcast frame. The switch receives this frame on Port 1. As the frame is received, the switch classifies it. The frame is untagged, so the switch classifies it as belonging to the VLAN that Port 1 is assigned to, the Red VLAN.

2. At the same time, the switch adds the source MAC address of the frame and the VLAN associated with port 1 to its Source Address Table in FDB ID 2. In this fashion it learns that station R1 is located out Port 1.

3. Once the frame is classified, its destination MAC address is examined. The switch discovers that the frame is a broadcast, and treats it as it would any other unknown destination MAC address. The switch forwards the frame out all ports in the Red VLAN’s Forwarding List except for the one that received the frame. In this case, the frame is sent to Ports 2 and 3.

   The second frame is a unicast, where station R2 responds to station R1’s broadcast.

4. Station R2, having received and recognized the broadcast from R1, transmits a unicast frame as a response. The switch receives this frame on Port 2. The switch classifies this new untagged frame as belonging to the Red VLAN.

5. The switch adds the source MAC address and VLAN for station R2 to its Source Address Table in FDB ID 2, and checks the Source Address Table for the destination MAC address given in the frame. The switch finds the MAC address and VLAN in this table, and recognizes that the MAC address and VLAN match for R1 is located out Port 1.

6. The switch examines its VLAN configuration information and determines that the frame for Red VLAN is allowed to be forwarded out Port 1 and that it must be sent in an untagged format.

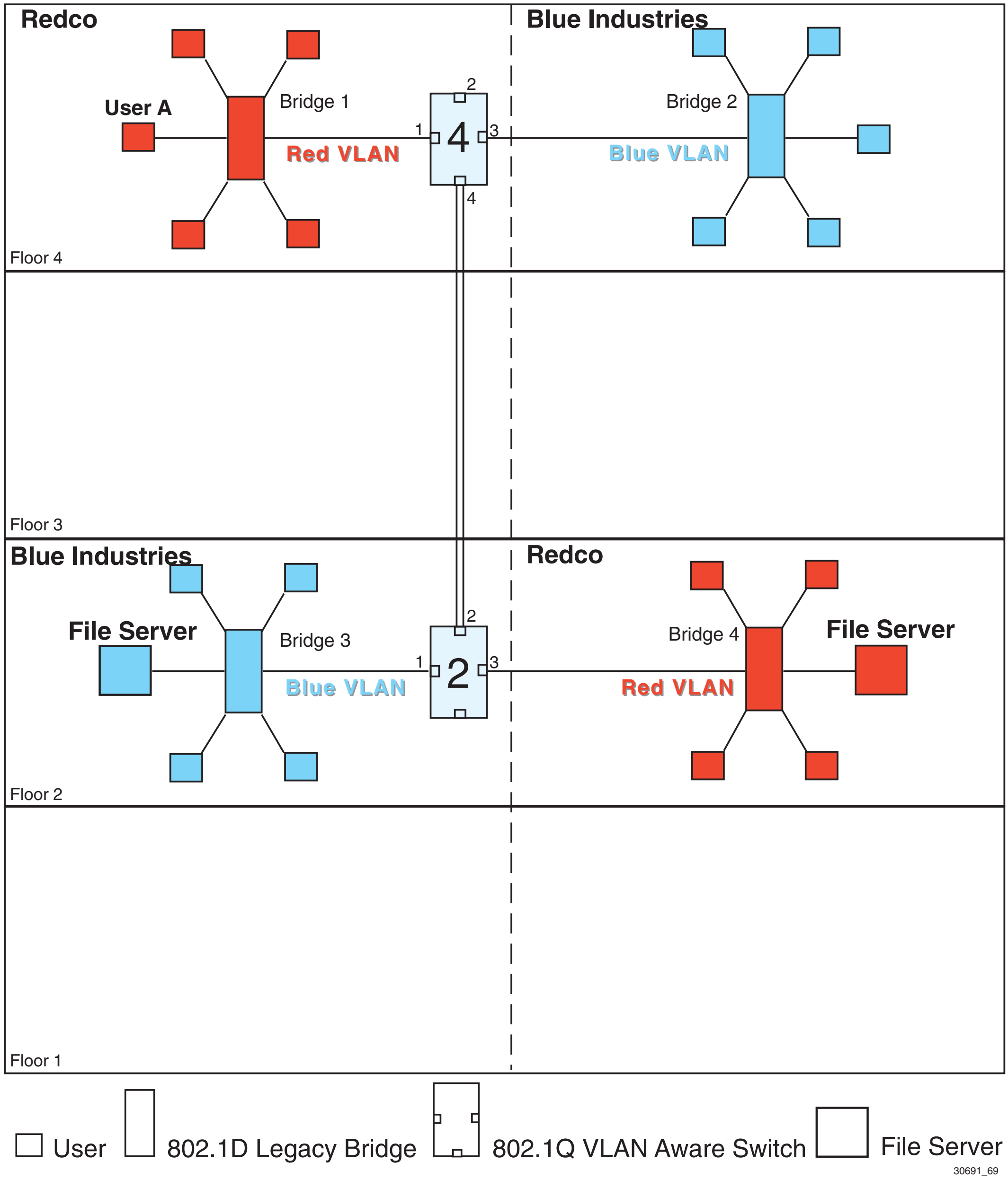
7. The switch forwards the frame out Port 1. Any other unicast transmissions between stations R1 and R2 will be handled identically.

12.13 EXAMPLE 2, VLANs ACROSS MULTIPLE SWITCHES

This second example investigates the steps that must be taken to set up VLANs across multiple 802.1Q VLAN switches. This includes the configuration and operation of trunk ports (port set for TAGGED frames only) between 802.1Q VLAN switches.

As shown in Figure 12-12, two companies, “Redco” and “Blue Industries,” share floors 2 and 4 in a building where the network infrastructure is supplied by the building owner. The objective is to completely isolate the network traffic of the two companies by limiting the user’s traffic through the ports of two switches, thus maintaining security and shielding the network traffic from each company. This example will show the use and configuration of a trunk connection and the creation of VLANs across multiple switches.

Figure 12-12 Example 2, VLANs Across Multiple Switches



12.13.1 Solving the Problem

To solve the problem in this example, the users are assigned to VLANs using Switch 4 and Switch 2 as shown in Figure 12-12. Redco users are assigned to the Red VLAN and Blue Industries users to the Blue VLAN. The following information shows how Switch 4 and Switch 2 are configured to create the two VLANs to isolate the users of the two companies from one another on the network using the existing infrastructure.

Switch 4

Switch 4 is set as follows:

1. Two VLANs are added to the list of VLANs in the Static VLAN Configuration screen. An FDB ID is automatically assigned to each VLAN. In this example, the following VLANs are created:

   - VLAN ID 2, FDB ID 2, with a VLAN Name of Red
   - VLAN ID 3, FDB ID 3, with a VLAN Name of Blue

   Because the VLANs are assigned to two separate FDB IDs, the users on VLAN ID 2 and VLAN ID 3 cannot communicate with each other.

2. The Egress type for both VLAN ID 2, Port 1, and VLAN ID 3, Port 3, are set to UNTAGGED using the Static VLAN Egress Configuration screen. This means that these ports will transmit only untagged VLAN frames.

3. Ports 1 and 3 are configured as follows using the VLAN Port Configuration screen:

   - Port 1 is set as follows:

     PVID: 2
     Acceptable Frame Types: ADMIT ALL FRAMES
     Ingress Filtering: ENABLED
     GVRP Status: DISABLED

   - Port 3 is set as follows:

     PVID: 3
     Acceptable Frame Types: ADMIT ALL FRAMES
     Ingress Filtering: ENABLED
     GVRP Status: DISABLED

   This causes the switch to classify all untagged frames received as belonging to the VLAN specified by each port PVID and to replace the previous PVID information in the port VLAN List with the new PVID information. This makes Port 1 part of the Red VLAN, Port 3 part of the Blue VLAN, and both are set to the VLAN frame format of untagged.

4. Port 4 is configured as a trunk port by setting the Egress type for both VLAN ID 2, Port 4 and VLAN ID 3, Port 4 to TAGGED using the Static VLAN Egress Configuration screen. This means that these ports will only transmit tagged VLAN frames.
   - Port 4, Egress: TAGGED
5. Port 4 is configured as follows using the VLAN Port Configuration screen:
   - Port 4 is set as follows:

     PVID: 1
     Acceptable Frame Types: ADMIT TAGGED FRAMES ONLY
     Ingress Filtering: ENABLED
     GVRP Status: ENABLED

   Port 4 is set as a trunk port and all frames forwarded out this port are forwarded as tagged frames. By default the port remains as a member of the Default VLAN. With the original classification information inserted in the frame Tag Header, the receiving switch will maintain the original frame classification. GVRP is enabled on this port and will support dynamic VLANs created by GVRP.

Switch 2

Switch 2 is set as follows:

1. Two VLANs are added to the list of VLANs in the Static VLAN Configuration screen. An FDB ID is automatically assigned to each VLAN. In this example, the following VLANs are created:
   - VLAN ID 2, FDB ID 2, with a VLAN Name of Red
   - VLAN ID 3, FDB ID 3, with a VLAN Name of Blue
2. The Egress type for both VLAN ID 3, Port 1, and VLAN ID 2, Port 3, are set to UNTAGGED using the Static VLAN Egress Configuration screen. This means that these ports will transmit only untagged VLAN frames.
3. Ports 1 and 3 are configured as follows using the VLAN Port Configuration screen:
   - Port 1 is set as follows:

     PVID: 3
     Acceptable Frame Types: ADMIT ALL FRAMES
     Ingress Filtering: ENABLED
     GVRP Status: DISABLED

- Port 3 is set as follows:

  PVID: 2
  Acceptable Frame Types: ADMIT ALL FRAMES
  Ingress Filtering: ENABLED
  GVRP Status: DISABLED

  This causes the switch to classify all untagged frames received as belonging to the VLAN specified by each port PVID and to replace the previous PVID information in the port VLAN List with the new PVID information. This makes Port 1 part of the Blue VLAN, Port 3 part of the Red VLAN, and both are set to the VLAN frame format of untagged.

4. Port 2 is configured as a trunk port by setting the Egress type for both VLAN ID 2, Port 2, and VLAN ID 3, Port 2, to TAGGED using the Static VLAN Egress Configuration screen. This means that these ports will only transmit tagged VLAN frames.

   - Egress: Port 2: TAGGED

5. Port 2 is configured as follows using the VLAN Port Configuration screen:

   - Port 2 is set as follows:

     PVID: 1
     Acceptable Frame Types: ADMIT TAGGED FRAMES ONLY
     Ingress Filtering: ENABLED
     GVRP Status: ENABLED

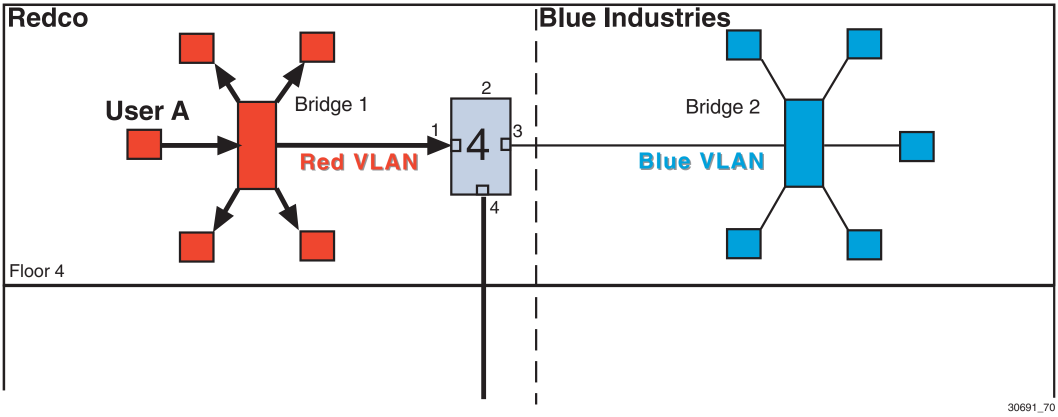
   Port 2 is set as a trunk port and all frames forwarded out this port are forwarded as tagged frames. By default the port remains as a member of the Default VLAN. With the original classification information inserted in the frame Tag Header, the receiving switch will maintain the original frame classification. GVRP is enabled on this port and will support dynamic VLANs created by GVRP. The operation of GVRP is described in Appendix A.

12.13.2 Frame Handling

The following describes how, when User A attempts to log on to the File Server on Bridge 4, the frames from User A are classified on Switch 4 and traverse the network. In this example, the MAC address of User A is "Y" and the MAC address for the File Server is "Z". The following description includes illustrations to help understand how the frames flow through the network.

1. User A sends a frame with a Broadcast Destination Address in an attempt to locate the File Server. The frame is received on User A's port of Bridge 1 and, because the frame is a broadcast frame, it is transmitted out all ports of Bridge 1 as shown in Figure 12-13.

Figure 12-13 Bridge 1 Broadcasts Frames



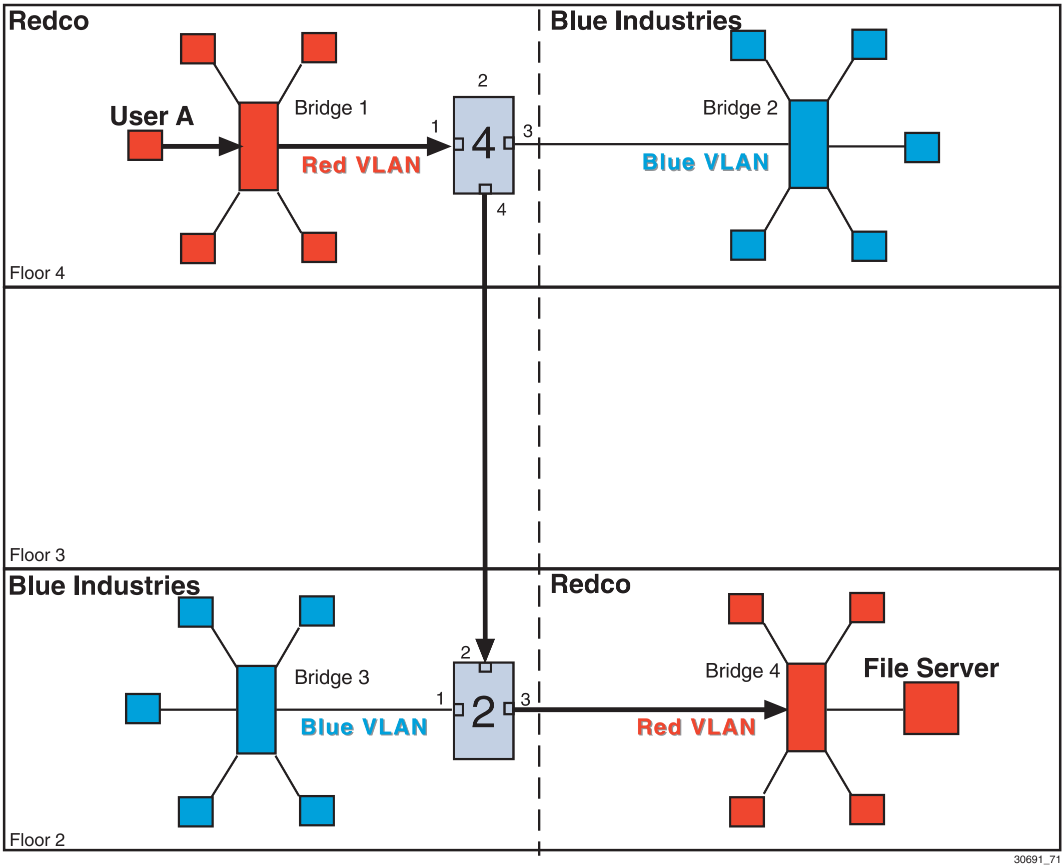
2. Switch 4 receives the frame from Bridge 1 and immediately classifies it as belonging to the Red VLAN. After the frame is classified, Switch 4 checks the Destination Address and, upon discovering that it is a Broadcast Destination Address, forwards the frame out all ports in the Red VLAN Forwarding List excluding Port 1, which received the frame. In this example, it is only Port 4.

   Switch 4 updates its Source Address Table in FDB ID 2 if it didn't already have a dynamic entry for MAC address "Y" in FDB ID 2. Because Switch 4 received the frame on Port 1, it does not forward the frame out that port, but does forward the frame to Port 4.

   The frame is transmitted to Switch 2 with a VLAN Tag Header inserted in the frame. The VLAN Tag Header indicates that the frame is classified as belonging to the Red VLAN. Figure 12-14 shows the path taken to this point to reach Switch 2.

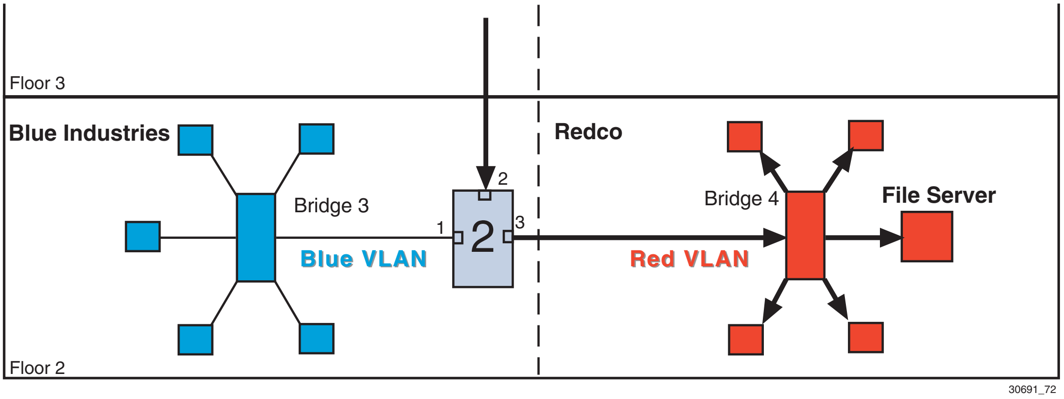
   The VLAN Tag Header is inserted because Switch 4, Port 4 is set to transmit tagged frames.

Figure 12-14 Transmitting to Switch 4



3. When Switch 2 receives the tagged frame on its Port 2, it checks the frame’s VLAN Tag Header and determines that the frame is classified as belonging to the Red VLAN, and that the frame is a broadcast frame. Switch 2 forwards the frame to all ports in the Red VLAN Forwarding List excluding Port 2, which received the frame. In this example, the only eligible port is Port 3, which connects to Bridge 4. Switch 2 checks its Forwarding List, which specifies that the VLAN frame type for that port is untagged. Switch 2 then updates its Source Address Table in FDB ID 2 for MAC address “Y” if necessary. The untagged frame is then transmitted out Port 3 to Bridge 4. Bridge 4 forwards the frame out all its ports because it is a broadcast frame, and the server receives it as shown in Figure 12-15.

Figure 12-15 Transmitting to Bridge 4



4. The File Server responds with a unicast frame to User A. All switches between the File Server and User A have an entry in their respective Source Address Tables identifying which port to use for forwarding the frame to User A, MAC address “Y” in FDB ID 2. All switches update their Source Address Tables for the File Server’s MAC address “Z” as the frame is forwarded through the switch fabric to User A. The 802.1D switches update their Source Address Tables based on the source MAC address and receive port and the 802.1Q switches update their databases based on the source MAC address, VLAN, and receive port.

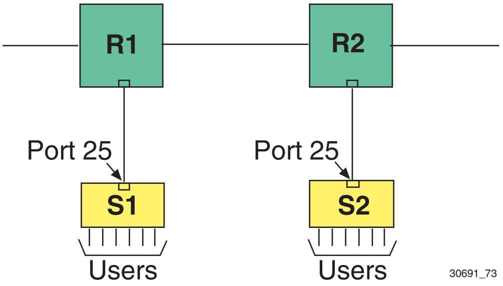
5. The frame from the File Server is received on Switch 2, and forwarded to Switch 1 as a tagged frame classified as belonging to the Red VLAN. Switch 1 removes the tag and forwards the frame to Bridge 1, which in turn forwards the frame out of the port attached to User A. All subsequent frames between User A and the File Server are forwarded through the switch fabric in the same manner.

12.14 EXAMPLE 3, FILTERING TRAFFIC ACCORDING TO A LAYER 4 CLASSIFICATION RULE

This example illustrates how to filter out broadcast transmissions at Layer 4 from other parts of a network.

In this example, illustrated in Figure 12-16, Switches S1 and S2 have already been configured and are operating. However, it was discovered that the Routing Information Protocol (RIP) broadcast frames from routers R1 and R2 were flooding the subnetwork of Switches S1 and S2.

Figure 12-16 Example 3, Filtering Traffic According to a Classification



12.14.1 Solving the Problem

To prevent the RIP broadcasts from flooding the users terminals connected to S1 and S2, a new VLAN will be added to each switch, but not assigned to any ports (creating a Null VLAN). Then each switch will be configured with a Layer 4 classification rule that will classify each RIP broadcast frame received on Port 25 of each switch to the Null VLAN. Since the Null VLAN is not associated with any ports, the frame will be dropped and not transmitted out any port.

In this example, the switches have already been configured and operating. The following covers only those steps needed to configure each switch to eliminate the problem.

Switches 1 and 2

Each switch is set as follows:

1. A VLAN is added to the list of VLANs in the Static VLAN Configuration screen and assigned to an FDB ID. In this example, the switch is set as follows:
   - VLAN ID 99, FDB ID 99, with a VLAN Name of Null VLAN

2. The VLAN Classification Configuration screen is used to configure the switch to detect and classify the incoming RIP broadcast frames on Port 25 to the Null VLAN. Since the Null VLAN is not assigned to any port, the frame is dropped (not transmitted out any port). The VLAN Classification Configuration screen is set as follows:

- VID: 99
- Classification: Dest UDP Port
- IP UDP Port: 520

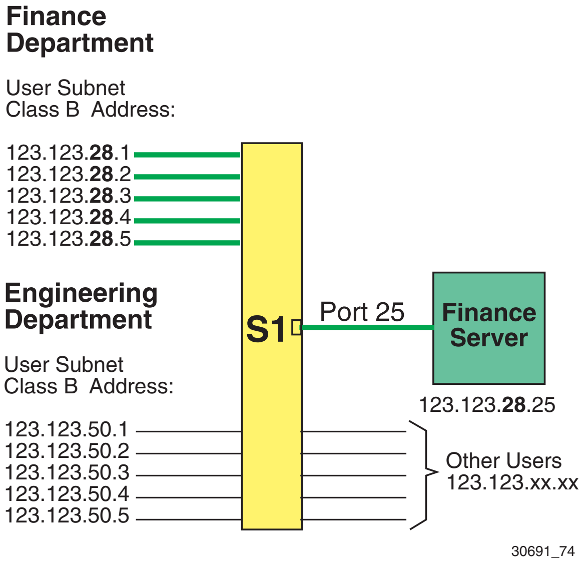
Port 520 is a well known port number used by RIP.

12.15 EXAMPLE 4, SECURING SENSITIVE INFORMATION ACCORDING TO SUBNET

The ABC Company wants to confine the sensitive information being transmitted by their Finance Department to its users only.

In this example, illustrated in Figure 12-17, the users in the Finance Department are members of the Finance VLAN and are also on subnet 28 as shown in **bold** type.

Figure 12-17 Example 4, Securing Traffic to One Subnet



12.15.1 Solving the Problem

In this example, Switch 1 (S1) has already been configured and is operating.

To isolate the Finance Department traffic, Subnet 28 will be isolated from the Engineering Department subnet 50 and other users on the company’s network (123.123.xx.xx).

The following covers only those steps needed to configure the switch to solve the problem.

Switch 1

To isolate the network traffic of the Finance Department to the users on the Finance VLAN (20), which are on subnet 28, S1 will be configured as follows using the VLAN Classification Configuration screen:

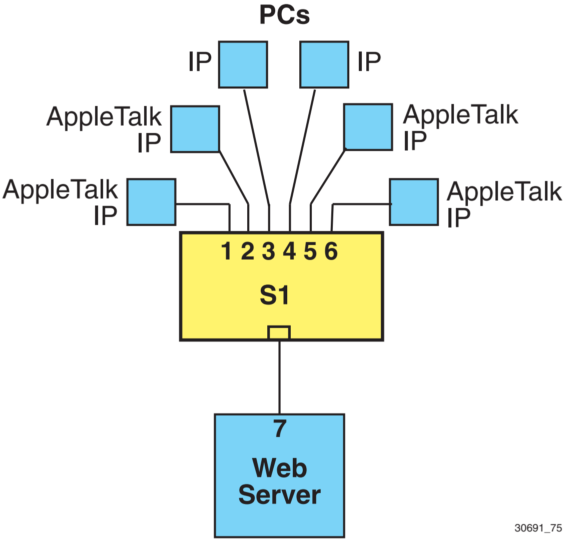
- VID: 20
- Classification: Bil IP Address
- IP Address: 123.123.28.0
- Data Mask: 255.255.255.0

As a result of this setting, any frame with a source or destination IP address of 123.123.28.xx (where xx can be a value of 0 to 255) will be classified to the Finance VLAN (20) and will remain within subnet 28. Any frame from another network or subnet will not be allowed access to subnet 28 because of the datamask 255.255.255.0.

12.16 EXAMPLE 5, USING DYNAMIC EGRESS TO CONTROL TRAFFIC

In this simple example (Figure 12-18), assume that there are four ports on the SmartSwitch device attached to PCs supporting both protocols AppleTalk (809B and 80F3) and IP. Two PCs support IP only. The AppleTalk frame traffic is to be contained so only the users running the AppleTalk protocol can communicate with each other and not flood the network with AppleTalk frames. However, all users are to have access to a web server connected to port 7.

Figure 12-18 Example 5, Dynamic Egress Application



Solving the Problem

In this example, Switch 1 (S1) has already been configured with a default VLAN 0001 associated with FDB ID 0001 as the PVID on all ports.

The following additional steps are required to configure the switch to solve this problem.

1. Define a new VLAN (VLAN ID 2) and filtering database (FDB ID 2) using the Device VLAN Configuration screen.
2. Create a Layer 2 rule to associate the protocol AppleTalk 809B and 80F3 to VLAN ID 2 (VID 2) using the VLAN Classification Configuration screen. This rule is assigned to all ports.
3. Enable the Dynamic Egress control on VLAN 2 using the Network Tools command (**dynamic_egress enable 2**).

With the above configuration, an AppleTalk frame received on any port will be classified into VLAN 2 (the AppleTalk VLAN), and the Port VLAN List of that port is updated to include VLAN 2.

For instance, if port 1 or 2 is connected to a new AppleTalk user, the AppleTalk frames received on that port are dynamically associated with VLAN 2 and VLAN 2 is added to the Port VLAN List of that port. The Port VLAN List contains a list of all VLANs whose frames can be transmitted out that port.

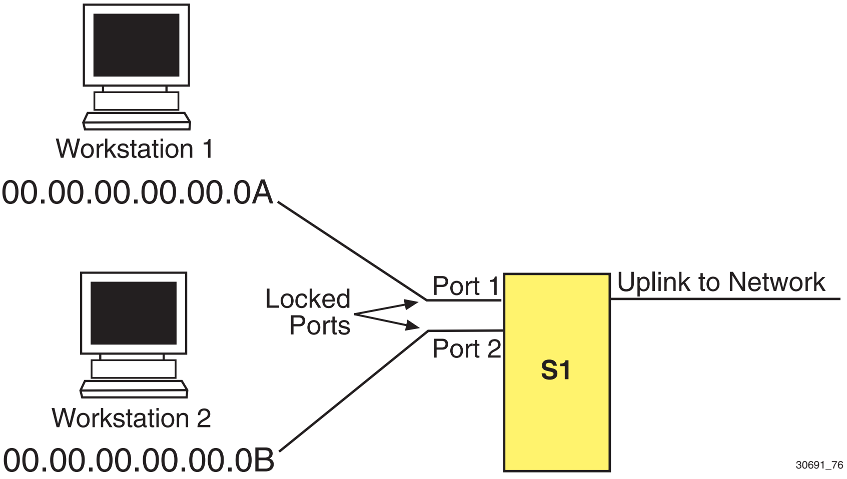
In this example, the AppleTalk traffic is routed only to AppleTalk users (ports 1, 2, 5, and 6), while IP traffic is allowed to be seen by IP users (ports 3, 4, and 7) and by IP/AppleTalk users (ports 1, 2, 5, and 6).

12.17 EXAMPLE 6, LOCKING A MAC ADDRESS TO A PORT USING CLASSIFICATION RULES

The following example illustrates how to add security by "locking" an individual MAC address to a port on the SmartSwitch device (S1). This would typically be done to ensure that only a particular device can gain access to the network from a specific port. Traffic received by the switch from any MAC address other than the one assigned to the "locked" port will be discarded.

In this example, illustrated in Figure 12-19, Switch S1 will be configured to lock ports 1 and 2 to the source address 00.00.00.00.00.0A and 00.00.00.00.00.0B of Workstation 1 and 2, respectively.

Figure 12-19 Example 6, Locking Ports According to Classification Rule



12.17.1 Solving the Problem

Switch S1 needs to be configured with two 802.1Q VLANs. Since the switch, by default, already has one VLAN created (the Default VLAN), only one new VLAN will need to be created. In this example, the new VLAN will be named the Red VLAN.

The objective here is to configure S1 so that when it receives a frame on Port 1 from MAC address 00.00.00.00.00.0A, the frame is classified into the Red VLAN. When S1 receives a frame on Port 1 from a MAC address other than 00.00.00.00.00.0A, the frame is associated with the Default VLAN. To accomplish this, S1 is configured so that the frames originating from the Red VLAN are eligible to be forwarded out the desired ports. The frames associated with the Default VLAN are not forwarded to any ports and are discarded by S1. Frames received on Port 2 will be handled in the same way except that S1 will only allow frames with the MAC address 00.00.00.00.00.0B frames to be forwarded out the desired ports and discard all other frames received on Port 2 that are not MAC address 00.00.00.00.00.0B frames.

This is accomplished using the screens as follows:

- The Static VLAN Configuration screen to create one VLAN, which will be named Red VLAN in this example.
- The Static VLAN Egress Configuration screen to set Ports 1 and 2 to transmit only untagged frames and add them to the VLAN Egress list of the switch.
- The Static VLAN Egress Configuration screen to remove all ports from the Default VLAN List.
- The VLAN Port Configuration screen to associate Ports 1 and 2 with Red VLAN and enable the port to receive all frames.
- The VLAN Classification Configuration screen to create two src MAC address classification rules and assign them to the appropriate new VLAN.
- The Protocol Ports Configuration screen to assign the new classification rules to Ports 1 and 2 and add the new VLANs to their port VLAN forwarding list.

Switch 1

To secure Port 1, you would configure Switch 1 as follows:

1. Create the static Red VLAN and add it to the module VLAN list by entering the following settings using the Static VLAN Configuration screen:

   - VLAN ID: 2
   - VLAN NAME: Red

2. Assign Port 1 and 2 to the Red VLAN and set the ports to handle untagged frames as follows:
   - The Red VLAN is selected from the Static VLAN Configuration screen to display the Static VLAN Egress Configuration screen.
   - The following are set using the Static VLAN Egress Configuration screen:

     – Port 1, Egress: UNTAGGED

     – Port 2, Egress: UNTAGGED

     No other ports are assigned to the Red VLAN and the exiting ports are left in the default setting of NO.
3. Remove all ports from the Default VLAN Egress List as follows:
   - The Default VLAN is selected from the Static VLAN Configuration screen to display the Static VLAN Egress Configuration screen. The following is set using the Static VLAN Egress Configuration screen:

     SET ALL PORTS: NO

   This configuration setting will cause the untagged frames sent to the Default VLAN from Ports 1 and 2 to be dropped because Ports 1 and 2 have been deleted from the Egress list of the Default VLAN.
4. Create two source (src) MAC address classification rules and apply them to the Red VLAN (VID 2), the following settings are entered using the VLAN Classification Configuration screen:

   For the Red VLAN and Port 1:
   - VID: 2
   - Classification: src MAC Address
   - Subclassification/MAC Address: 00.00.00.00.00.0A
   - ADD the rule. It will display in the top half of the VLAN Classification Configuration screen.

5. Enter the following settings on the Protocol Port Configuration screen to assign two src MAC address classification rules to Port 1 and add the classification to the Port VLAN List of Port 1:

- Port 1: YES to assign the classification rule to Port 1
- SET PORTS TO VLAN FORWARDING: YES to add the VLAN and classification rule to the Port VLAN List of Port 1

For the Red VLAN and Port 2 set the following:

- VID: 2
- Classification: src MAC Address
- Subclassification/MAC Address: 00.00.00.00.00.0B
- ADD the rule. It will display in the top half of the VLAN Classification Configuration screen.

6. Enter the following settings on the Protocol Port Configuration screen to assign the new classification rule to Port 2 and add the classification to the Port VLAN List of Port 2:

- Port 2: YES to assign the classification rule to Port 2
- SET PORTS TO VLAN FORWARDING: YES to add the VLAN and classification rule to the Port VLAN List of Port 2.

A

Generic Attribute Registration Protocol (GARP)

This appendix describes the switch operation when its ports are operating under the Generic Attribute Registration Protocol (GARP) application – GARP VLAN Registration Protocol (GVRP).

NOTE: There is a global setting for GVRP that is enabled by default. Access to these settings is only available through a MIB.

A.1 OVERVIEW

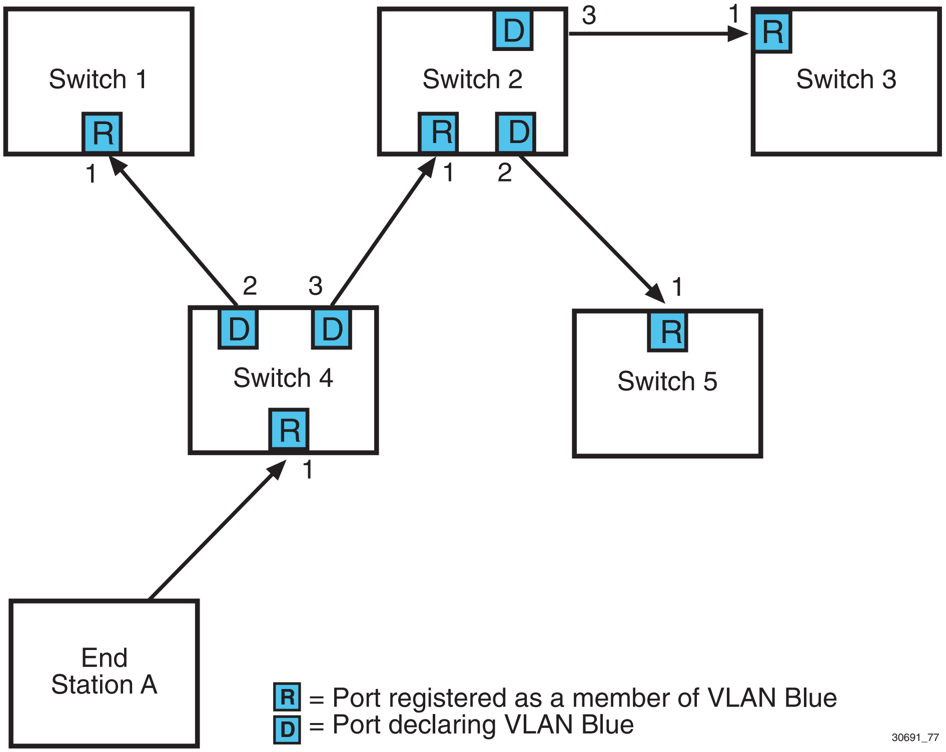
The process of the forwarding decision and tagging frames is the same as for 802.1Q as described in Chapter 12. However, the GVRP protocol frames will not have a tag even when transmitted out an 802.1Q Trunk Port.

The purpose of GVRP is to dynamically create VLANs across a switched network. When a VLAN is declared, the information is transmitted out GVRP configured ports on the switch in a GARP formatted frame using the GVRP multicast MAC address. A switch that receives this frame, examines the frame, and extracts the VLAN IDs. GVRP then creates the VLANs and adds the receiving port to its tagged member list for the extracted VLAN ID(s). The information is then transmitted out the other GVRP configured ports of the switch. Figure A-1 shows an example of how VLAN blue from end station A would be propagated across a switch network.

A.2 HOW IT WORKS

In Figure A-1, Switch 4, port 1 is registered as being a member of VLAN Blue and then declares this fact out all its ports (2 and 3) to Switch 1 and Switch 2. These two switches register this in the Port VLAN Lists of the ports (Switch 1, port 1 and Switch 2, port 1) that received the frames with the information. Switch 2, which is connected to Switch 3 and Switch 5 declares the same information to those two switches and the Port VLAN List of each port is updated with the new information, accordingly.

Figure A-1 Example of VLAN Propagation via GVRP



Configuring a VLAN on an 802.1Q switch creates a static GVRP entry. The entry will always remain registered and will not time out. However, dynamic entries will time-out and their registrations are removed from the member list if the end station A is removed. This ensures that if switches are disconnected, or if end stations are removed, the registered information remains accurate.

The end result is that the Port VLAN List of a port is updated with information about VLANs that reside off that port, even if the actual station on the VLAN is several hops away.

B

About IGMP

This appendix provides information about the following:

- IGMP Overview (Section B.1)
- Supported Features and Functions (Section B.2)
- Detecting Multicast Routers (Section B.3)

B.1 IGMP OVERVIEW

Internet Group Management Protocol (IGMP) is a multicast protocol used by routers. This protocol is supported by Enterasys Network SmartSwitches when operating in the 802.1Q mode to "snoop" the IGMP frames. The multicast information is gleaned from the IGMP frame and a filter is created to send the stream of data only to those end stations that will receive it.

IGMP queries are sent periodically from routers. An end station that will receive a multicast stream will send a "query response" back to the router. If the router does not receive any response from the end station, it stops forwarding the multicast streams to that station.

IGMP messages use an IP protocol number of 2. Routers send queries to the all-hosts group of 224.0.0.1. End stations send query responses to the multicast address of the stream they are requesting to receive.

Routers need to be discovered and all multicast packets need to be sent to all routers.

B.2 SUPPORTED FEATURES AND FUNCTIONS

The following lists the features and functions supported when using IGMP:

- Runs only when the switch is operating in the 802.1Q mode.
- Supports multiple multicast and non-multicast routers on the same VLAN.
- Supports stand alone multicast servers only if a router is present on the network.
- Multicast forwarding rate is dependent on the number of ports the multicast stream is forwarded to. More ports degrade the performance.
- Supports IGMP version 1 and 2 only. Default is version 2.
- Ports that are directly connected to routers are discovered dynamically through snooping for routing protocols.
- IGMP is enabled or disabled per VLAN, and not per port.

NOTE: Certain versions of firmware will not allow the switch to be a querier. Please check your release notes for further information. Refer to RFC 2236, Section 8, for more information on IGMP.

- The switch will “snoop” on all incoming multicast addresses to detect query responses, as well as queries. Query responses are sent to the multicast address detected in the stream from the host requesting to receive queries. The frame is an IP frame of protocol type 2. If the frame is a response frame, IGMP will take the multicast address and VLAN ID, and program a filter on the receive port. The response is then forwarded out upstream ports so that the router will receive it. Ports that receive queries are marked as upstream ports. It is assumed a router exists somewhere off this port, and responses are sent here. If the switch detects a router protocol on a port, that port is also marked as a router port. This keeps the switch from blocking traffic to other routers.

B.3 DETECTING MULTICAST ROUTERS

The location of a router needs to be known in order to forward IGMP report frames back to the router. The router(s) send multicast routing protocol frames which get flooded throughout the network. By snooping on these protocol, the switch will mark ports as connected to a router. The port is put in a “forward all” mode where all multicast frames will be flooded. This allows all types of IP multicast traffic (including IGMP streams) to go to the router.

There are many multicast routing protocols that the switch supports. These include the following:

- PIM version 1 and 2
- CBT (core based trees)
- MOSPF
- DVMRP

The routing protocols are detected as follows:

- All the multicast routing protocols have a destination address of 01-00-5E.
- DVMRP and PIM version 1 run over IGMP. If the IGMP frame type is not a REPORET, QUERY, OR LEAVE, then the frame is assumed to be one of these.
- PIM version 2 is IP protocol type 0x67.
- OSPF is IP protocol type 0x59. To detect that the frame is a multicast OSPF (MOSPF), the OSPF data must be looked at. The data starts after the IP header. Byte 31 (options) needs to be checked. If bit 2 is set (0x02 the MC bit), the frame is a MOSPF frame.
- CBT is IP protocol type 0x07.
- IGMP frames are detected by checking the IP protocol type. If the type is -x02, it is IGMP. The first byte following the IP header is the IGMP frame type and version. (Note that the lower 4 bits of the first byte in the IP header is the length of the IP header in 32 bit words) The version is always 1, so the entire byte (version +type) may be used to check the IGMP type as follows:

  0x11 = query

  0x12 = report version 1

  0x16 = report version 2

  0x17 = leave

Index

Numerics

1D Connection 12-6
1D Trunk 7-20
1Q Connection 12-6
1Q Trunk 7-20
802.1 Configuration Menu screen 6-2
802.1p Configuration Menu screen 8-2
802.1Q switching mode
  hierarchy of 3-2
802.1Q VLAN Configuration Menu screen 7-3
802.3ad Aggregator Details screen 5-41
  screen fields
    Admin Key 5-42
    Aggregator Instance 5-42
    Collector Max Delay 5-42
    Oper Key (Actor) 5-42
    Oper Key (Partner) 5-42
    System Identifier 5-42
    System Priority (Actor) 5-42
    System Priority (Partner) 5-42
802.3ad Aggregator screen 5-39
  screen fields
    AggInst 5-40
    NumPorts 5-40
    OperKey 5-40
    SysPri 5-40
802.3ad Main Menu screen 5-23
802.3ad Port Details screen 5-30
  screen fields
    ActorAdminKey 5-31
    ActorAdminState (hex) 5-32
    ActorOperKey 5-31
    ActorOperState 5-33–5-34
    ActorPort 5-31
    ActorPortPriority 5-31
    ActorSystemID 5-31
    ActorSystemPriority 5-31
    AttachedAggID 5-34
    LAGID 5-35
    PartnerAdminKey 5-34
    PartnerAdminPort 5-31
    PartnerAdminPortPriority 5-31
    PartnerAdminState (hex) 5-34
    PartnerAdminSysID 5-32
    PartnerAdminSysPriority 5-31
    PartnerOperKey 5-34
    PartnerOperPort 5-31
    PartnerOperPortPriority 5-31
    PartnerOperState 5-34
    PartnerOperSysID 5-32
    PartnerOperSysPriority 5-31
    Port Instance 5-31
    SelectedAggID 5-34
    STATS 5-35
802.3ad Port screen 5-27
  screen fields
    Aggregator 5-29
    MUX 5-29
    OperKey 5-29
    Port 5-29
802.3ad Port Statistics screen 5-36
  screen fields
    ActorChangeCount 5-38
    ActorChurnCount 5-38
    ActorChurnState 5-38
    AsyncTransCount 5-38
    IllegalRx 5-37
    LACPDUsRx 5-37
    LACPDUsTx 5-37
    LastRxTime(delta) 5-38
    MarkerPDUsRx 5-37
    MarkerPDUsTx 5-37
    MarkerResponsePDUsRx 5-37
    MarkerResponsePDUsTx 5-37

MuxReason 5-38
MuxState 5-38
PartnerChangeCount 5-38
PartnerChurnCount 5-38
PartnerChurnState 5-38
Port Instance 5-37
PsyncTransCount 5-38
RxState 5-37
UnknownR 5-37
802.3ad System screen 5-43
screen fields
Number of Aggregators 5-44
Number of Ports 5-44
System Identifier 5-44

A

Acceptable Frame Type
setting of 7-21
Access Control List screen 4-23
screen fields
Access Control Lists 4-24
IP Addresses 4-24
MASK 4-25
Access Policy 4-20
Advertised ability
setting of 5-12
Assigning Ports to a VID/Classification
all at a time 7-13, 7-37
one or more at a time 7-13, 7-37
Assigning VID/Classification to Port VLAN Lists 7-38
Authentication Server 3-16
Authenticator 3-15

B

Broadcast Suppression Configuration screen 5-44
screen fields
Peak Rate 5-46
PORT # 5-45
Reset Peak 5-46
Threshold 5-46
Time Since Peak 5-46
Total RX 5-45
Built-in Commands
use of 11-2

C

Classification List 7-24, 8-19
Classification Precedence Rules 7-29
Classification Rule
filtering traffic according to 12-32
CLEAR COUNTERS command
how to use 3-4
COM port 4-13
Command field 1-6
Command set 11-2
Configuration 12-7
VLAN Spanning Tree 6-8
VLAN Spanning Tree ports 6-11
Controlling Traffic
example of 11-39
Current VLAN Configuration screen 7-14
screen fields
FDB ID 7-15
Ports on Egress 7-16
VLAN ID 7-15
VLAN Type 7-15
Current VLAN Egress Configuration screen 7-16
screen fields
Egress 7-17
Port 7-17
Cursor movement 1-3

D

Default VLAN 12-5
Device Configuration Menu screen 4-2
Device Date
setting the 4-11
Device Menu screen 3-7
Device Statistics Menu screen 10-1
Device Time
setting the 4-12
Display field 1-5
Document conventions xx
Dynamic Egress
example of use 11-39

E

EAP 3-15
EAP (Port) Configuration screen 3-35
  screen fields
    Authentication State 3-36
    Backend State 3-37
    Force Reauth 3-39
    Initialized Port 3-39
    Maximum Requirements 3-39
    Port 3-36
    Port Control 3-38
EAP Authenticator Statistics screen 3-44
  screen fields
    CLEAR COUNTERS 3-46
    Frame Source 3-46
    Frame Version 3-46
    Invalid Frames Rx 3-46
    Length Error Frames Rx 3-46
    Logoff Frames Rx 3-45
    Port Number 3-46
    Request Frames Tx 3-46
    Request Id Frames Tx 3-46
    Response Frames Rx 3-46
    Response Id Frames Rx 3-46
    Start Frames Rx 3-45
    Total Frames Rx 3-45
    Total Frames Tx 3-45
EAP Diagnostic Statistics Screen 3-47
EAP Diagnostic Statistics screen
  screen fields
    Access Challenges 3-49
    Auth Failures 3-49
    Auth Successes 3-49
    CLEAR COUNTERS 3-50
    Enters Authenticating 3-48
    Enters Connecting 3-48
    Fail Authenticating 3-48
    Logoffs Authenticated 3-49
    Logoffs Authenticating 3-48
    Logoffs Connecting 3-48
    Non-NAK resp From Supp 3-49
    Other Requests To Supp 3-49
    Port Number 3-50
    Reauths Authenticated 3-49
    Reauths Authenticating 3-48
    Responses (Read-Only) 3-49
    Starts Authenticated 3-49
    Starts Authenticating 3-48
    Success Authenticating 3-48
    Timeouts Authenticating 3-48
EAP Session Statistics screen 3-42
  screen fields
    CLEAR COUNTERS 3-44
    Port Number 3-44
    Session Authenticate Method 3-43
    Session Terminate Cause 3-43
    Session Time 3-43
    Session User Name 3-44
    SessionFramesRx 3-43
    SessionFramesTx 3-43
    SessionID 3-43
    SessionOctetsRx 3-43
    SessionOctetsTx 3-43
EAP Statistics Menu screen 3-40
Egress Types on Ports
  setting of 7-13
Ethernet Interface Configuration screen 5-4
  screen fields
    Config 5-6
    Duplex 5-6
    FDX FC 5-6
    HDC FC 5-7
    Intf 5-5
    Link 5-6
    port 5-5
    Port Type 5-5
    Speed 5-6
Ethernet Port Configuration screen 5-7
  screen fields
    Advertised Ability 5-10
    Auto-Negotiation State 5-9
    Default Duplex 5-9
    Default Speed 5-9
    Full Duplex Flow Control 5-11
    Half Duplex Flow Control 5-11
    Interface 5-9
    Physical Port 5-9
    SAVE TO ALL PORTS 5-11
Event message field 1-5

Examples 12-21
Extensible Authentication Protocol 3-15

F

FID. *See* Filtering Database ID
Fields
  command 1-6
  display 1-5
  event message 1-5
  input 1-5
  selection 1-5
  types 1-5
Filtering Database 12-5
Filtering Database ID 12-5
Filtering Network Traffic According to a Layer 4 Classification Rule 12-32
Flash Download Configuration screen 4-30
  screen fields
    Download File Name 4-33
    Download Method 4-32
    Download Server IP 4-33
    Download Status 4-33
    Last Image File Name 4-33
    Last Image Server IP 4-33
    Reboot After Download 4-33
    TFTP Gateway IP Addr 4-33
Forwarding list 12-5
  customizing 12-8
Fragmentation 4-7
Frames
  tagged 12-5, 12-10
  untagged 12-5, 12-10

G

Gateway IP address
  setting the 4-10
General Configuration screen 4-4
  COM port
    configuring 4-13
  Default Gateway
    setting the 4-10
  IP Address
    setting the 4-8
  screen fields
    Agg Mode 4-7
    Application 4-6
    Clear NVRAM 4-7
    Com 4-6
    Default Gateway 4-5
    Device Date 4-5
    Device UpTime 4-6
    IP Address 4-5
    IP Fragmentation 4-7
    MAC Address 4-5
    Module Name 4-5
    Module Time 4-6
    Operational Mode 4-6
    Screen Lockout Time 4-6
    Screen Refresh Time 4-6
    Subnet Mask 4-5
    Telnet 4-7
    TFTP Gateway IP Addr 4-5
    WebView 4-7
Getting help 1-7
GVRP
  enabling or disabling on port 7-21
  purpose of A-1

H

Hierarchy
  802.1Q switching mode 3-2
Host Access Control Authentication (HACA)
  how to use 3-12
Host data port 12-12, 12-14
HSIM/VHSIM Configuration screen 5-13
Hybrid 7-20

I

IGMP
  detecting multicast routers when using B-3
  features and functions supported B-2
  overview of B-1
IGMP/VLAN Configuration screen 9-3
  screen fields
    IGMP State 9-7
    IGMP Version 9-4

Interface Robustness 9-5
Last Member Query Interval 9-5
Multicast Pool Size 9-6
Querier Address 9-6
Querier Expire Time 9-6
Querier Uptime 9-6
Query Interval 9-5
Query Response Time 9-5
Switch Query IP 9-6
VLAN ID 9-7
Ingress Filtering
enabling or disabling of port 7-21
Input field 1-5
Interface Statistics screen 10-5
screen fields
Address 10-7
Admin Status 10-8
CLEAR COUNTERS 10-8
InDiscards 10-7
InErrors 10-7
InNonUnicast 10-7
InOctets 10-6
Interface 10-6
Interface (command) 10-8
InUnicast 10-7
InUnknownProtos 10-7
Last Change 10-8
MTU 10-8
Name 10-6
Oper Status 10-8
OutDiscards 10-7
OutErrors 10-7
OutNonUnicast 10-7
OutOctets 10-7
OutQLen 10-7
OutUnicast 10-7
speed 10-8
IP Address 4-5
IP Fragmentation 4-7
enabling/disabling of 4-16

K

Keyboard conventions 1-6

L

Layer 3 Extensions Menu screen 9-1
Link Aggregation Menu screen. *See* 802.3ad Main Menu screen
Lists
Forwarding 12-5
Port VLAN 12-5
Local Management
clearing counters 3-4
exiting from 3-3
navigating the screens 3-1
paging to next or previous screen 3-4
requirements 1-3
screen elements 1-4
Local Management Chassis/Module Password screen 3-4–3-5
Local Management screens
selection of 3-3
Local management. *See* managing the switch

M

MAC Locking 11-15
MAC Port Configuration screen 3-50
screen fields
Authentication State 3-51
Force Reauth 3-52
Initialize Port 3-52
Port # 3-51
Port Enable 3-51
SET ALL PORTS 3-52
MAC Supplicant Configuration screen 3-52
screen fields
Duration 3-53
Initialize Supplicant 3-54
MAC Address 3-53
Port 3-53
Reauthenticate Supplicant 3-54
Management agent 1-2
Management Terminal
COM port connection of 2-1–2-2
setup of 2-1, 2-3
Managing the switch 12-11
when configured with VLANs 12-12

when not configured with VLANs 12-12
Module Login Passwords screen (Security) 3-25
Access Policy 3-26
Password 3-26
Restrict NVRAM Passwords from Upload/Download 3-26
Switch 8 3-26
Module Time 4-6
Moving the cursor 1-3

N

Name Services Configuration screen 3-31
Names Services Configuration screen
screen fields
Name Services 3-32
Secure Harbour IP 3-32
Switch Name 3-32
Web Authentication 3-32
Navigating screens 3-1
Network management
in-band 1-3
out-of-band 1-3
Network Tools
built-in commands 11-2
alias 11-4
arp 11-6
arp_learn 11-7
atm_stp_state 11-3
bridge 11-7
cdp 11-8
defroute 11-8
dynamic_egress 11-9
ev 11-10
gigabit_port_mode 11-12
igmpv3_drop 11-12
lg_frame_admin 11-13
link_trap 11-14
loopback_detect 11-14
MAC lock 11-15
netstat 11-18
non_bridge_if_num 11-19
passiveStp 11-20
ping 11-20
policy 11-21
radius 11-23
rate_limit_mode 11-26
reset 11-27
sat_size 11-28
show 11-28, 11-32
soft_reset 11-30
stpEdgePort 11-30
stpForceVersion 11-31
stpPointToPointMAC 11-33
stpPort 11-34
stpRealTimeMsgAge 11-34
suppress_topology_traps 11-35
telnet 11-35
timed_reset 11-36
timed_soft_reset 11-36
traceroute 11-37
vrrpPort 11-38
description of 11-1
functional CLI commands
dynamic_egress 11-9
vrrpPort 11-38
special commands 11-3, 11-40
done, quit, or exit 11-40
Network Tools Help screen 11-2
Network Traffic
filtering 12-32
NEXT command
how to use 3-4
NVRAM
clearing of 4-15

P

PAE 3-15
Password screen (Local Management) 3-4
Port Access Authentication 3-15
Port Configuration Menu screen 5-2
Port mode
1D Trunk 7-20
1Q Trunk 7-20
changing the 7-20
Hybrid 7-20
Port Priority Configuration screen 8-4

screen fields
Port 8-6
Port Redirect Configuration screen 5-15
screen fields
Destination Port 5-16
Destination Port [n] 5-17
Frame Format (Read-Only) 5-17
Frame Format (Selectable) 5-17
Redirect Errors 5-17
Redirect Errors (Toggle) 5-17
Source Port 5-16
Source Port [n] 5-17
Status 5-17
Port Security
setup example 12-36
Port VLAN list 12-5
Port Web Authentication 3-15
Ports
setting Egress types on 7-13
PREVIOUS command
how to use 3-4
Priority Classification Configuration screen 8-16
screen fields
ADD 8-18
Classification 8-18
Classification (top of screen) 8-17
DEL ALL/DEL MARKED 8-18
Description (top of screen) 8-17
PID 8-17–8-18
Protocol Port Configuration screen 8-32
screen fields
Classification Rule 8-33
Classify 8-33
Policy Override 8-6
Port 8-33
Priority 8-6
Set 8-6
SET ALL PORTS 8-33
Protocol Port Configuration screen (VLAN) 7-34
screen fields
Classification Rule Field 7-36
Classify 7-36
Port 7-36
SET ALL PORTS 7-36
SET PORTS TO VLAN FORWARDING 7-37
PVID
assigning to port 7-20
PVST Port Configuration screen 6-11
screen fields
Corresponding idDescr 6-12
Corresponding ifindex 6-12
Port # 6-12
Port Designated Bridge 6-12
Port Designated Cost 6-13
Port Designated Port 6-13
Port Designated Root 6-12
Port Enable 6-13
Port Forward Transmissions 6-13
Port Path Cost 6-13
Port Priority 6-13
Port State 6-13
STP Vlan ID 6-13
PWA 3-15

Q

Queueing Mode
setting of 8-15

R

Radius 3-15
Radius Configuration screen 3-27
screen fields
Auth Port 3-29
IP Address 3-29
Last Resort Action/Local 3-29
Last Resort Action/Remote 3-29
Radius Client 3-29
Retries 3-28
Secret 3-29
Timeout 3-28
Radius Server
multiple access for 3-12
type access levels for 3-12
Rate Limiting
changing/deleting port configuration for 8-43
configuration ports for 8-41

  - example of 8-44
  - more about 8-44
- Rate Limiting Configuration screen 8-37
  - screen fields
    - ADD 8-41
    - DEL ALL/DEL MARKED 8-41
    - Direction 8-39–8-40
    - Dropped Events 8-39
    - Feature 8-39
    - Kbps 8-41
    - Max Traffic Rate 8-39
    - Port 8-38
    - Port Number 8-39
    - Port Type 8-39
    - Priority List 8-38, 8-40
- Redirect Configuration Menu screen 5-13
- Related manuals xx
- Remote management. *See* managing the switch
- RMON Statistics screen 10-9
  - screen fields
    - 1024 – 1518 Octets 10-12
    - 128 – 255 Octets 10-11
    - 256 – 511 Octets 10-11
    - 512 – 1023 Octets 10-11
    - 64 Octets 10-11
    - 65 – 127 10-11
    - 65 – 127 Octets 10-11
    - Broadcast Pkts 10-10
    - CLEAR COUNTERS 10-12
    - Collisions 10-10
    - CRC Align Errors 10-10
    - Data Source 10-10
    - Drop Events 10-10
    - Fragments 10-11
    - fragments 10-11
    - Index (command) 10-12
    - Jabbers 10-11
    - Multicast Pkts 10-10
    - Oversized Pkts 10-11
    - Owner 10-10
    - RMON index 10-10
    - Status 10-10
    - Total Octets 10-11
    - Total Packets 10-11
    - Undersized Packets 10-10
- Rules
  - Classification Precedence 7-29

S

- Screen fields
  - command fields 1-6
  - display fields 1-5
  - event message field 1-5
  - input fields 1-5
  - selection fields 1-5
- Screen Lockout Time
  - setting the 4-12
- Screen Refresh Time
  - entering a 4-12
- Screens
  - 802.1 Configuration Menu screen 6-2
  - 802.1p Configuration Menu screen 8-2
  - 802.1Q VLAN Configuration Menu screen 7-3
  - 802.3ad Aggregator Details screen 5-41
  - 802.3ad Aggregator screen 5-39
  - 802.3ad Main Menu screen 5-23
  - 802.3ad Port Details screen 5-30
  - 802.3ad Port screen 5-27
  - 802.3ad Port Statistics screen 5-36
  - 802.3ad System screen 5-43
  - Access Control List screen 4-23
  - Broadcast Suppression Configuration screen 5-44
  - clearing counters 3-4
  - Current VLAN Configuration screen 7-14
  - Current VLAN Egress Configuration screen 7-16
  - Device Configuration Menu screen 4-2
  - Device Menu screen 3-7
  - Device Statistics Menu screen 10-1
  - EAP (Port) Configuration screen 3-35
  - EAP Authenticator Statistics screen 3-44
  - EAP Diagnostic Statistics Screen 3-47

EAP Session Statistics screen 3-42
EAP Statistics Menu screen 3-40
Ethernet Interface Configuration screen 5-4
Ethernet Port Configuration screen 5-7
exiting from 3-3
FLASH Download Configuration screen 4-30
General Configuration screen 4-4
hierarchy of 3-1
HSIM/VHSIM Configuration screen 5-13
IGMP/VLAN Configuration screen 9-3
Interface Statistics screen 10-5
Layer 3 Extensions Menu screen 9-1
Link Aggregation Menu screen. *See* 802.3ad
    Main Menu screen
MAC Port Configuration screen 3-50
MAC Supplicant Configuration screen 3-52
Module Login Passwords screen (Security) 3-25
Name Services Configuration screen 3-31
navigation of 3-1
Network Tools screen 11-1
paging to next or previous 3-4
Password screen (Local Management) 3-4
Port Configuration Menu screen 5-2
Port Priority Configuration screen 8-4
Port Redirect Configuration screen 5-15
Priority Classification Configuration
    screen 8-16
Protocol Port Configuration screen 8-32
Protocol Port Configuration screen
    (VLAN) 7-34
PVST Port Configuration screen 6-11
Radius Configuration screen 3-27
Rate Limiting Configuration screen 8-37
Redirect Configuration Menu screen 5-13
RMON Statistics screen 10-9
selection of 3-3
SNMP Community Names Configuration
    screen 4-18
SNMP Configuration Menu screen 4-17
SNMP Traps Configuration screen 4-21
Spanning Tree Configuration Menu screen 6-4
Spanning Tree Configuration screen 6-5
Spanning Tree Port Configuration screen 6-9
Static VLAN Configuration screen 7-6
Static VLAN Egress Configuration screen 7-11
Switch Statistics screen 10-3
System Authentication Configuration
    screen 3-33
System Resources Information screen 4-28
Traffic Class Configuration screen 8-10
Traffic Class Information screen 8-7
Transmit Queues Configuration screen 8-12
VLAN Classification Configuration screen 7-21
VLAN Port Configuration screen 7-17
VLAN Redirect Configuration screen 5-19

Security screens
  EAP (Port) Configuration screen 3-35
  EAP Authenticator Statistics screen 3-44
  EAP Statistics Menu screen 3-40
  MAC Port Configuration screen 3-50
  MAC Supplicant Configuration screen 3-52
  Name Services Configuration screen 3-31
  Passwords screen 3-25
  Radius Configuration screen 3-27
  System Authentication Configuration
    screen 3-33
Security, Ports
  setup example 12-36
Selection field 1-5
Set Ports to VLAN Forwarding 7-38
Setting the Module Login Password 3-27
Setup of
  management terminal 2-3
SNMP Community Names
  setting of 4-18
SNMP Community Names Configuration
    screen 4-18
  screen fields
    Access Policy 4-20
    Community Name 4-19
SNMP Configuration Menu screen 4-17
SNMP Traps Configuration screen 4-21
  screen fields
    Enable Traps 4-22
    Trap Community Name 4-22
    Trap Destination 4-22

trap table configuration 4-22
Spanning Tree Configuration Menu screen 6-4
Spanning Tree Configuration screen 6-5
screen fields
ADD ALL CONFIGURED VLAN 6-7
Age Time 6-6
Current STP Mode 6-7
Operation 6-7
Priority 6-7
VLAN 6-6
VLAN (Modifiable) 6-7
Spanning Tree Port Configuration screen 6-9
screen fields
Age Time 6-10
MAC Address 6-10
Number of Ports 6-10
PORT # 6-10
State 6-10
Status 6-10
STP Instance 6-10
Switch Address 6-10
Special commands
use of 11-3
Special Commands, Network Tools 11-40
Static VLAN Configuration screen 7-6
screen fields
ADD 7-8
DEL MARKED 7-8
FDB ID 7-7
VLAN ID 7-7
VLAN ID (bottom of screen) 7-8
VLAN Name 7-8
VLAN Name (bottom of screen) 7-8
Static VLAN Egress Configuration screen 7-11
FDB ID 7-12
screen fields
Egress 7-12
Port 7-12
SET ALL PORTS 7-12
VLAN ID 7-12
VLAN Name 7-12
Station 12-7
Strict 802.1p Queueing Mode
setting of 8-15
Subnet Mask 4-5, 4-9
Supplicant 3-16
Switch 12-7
Switch 8 Function
Enable/Disable 3-26
Switch Statistics screen 10-3
clearing counters 10-5
screen fields
CLEAR COUNTERS 10-5
Frames Fltrd 10-4
Frames Frwded 10-5
Frames Rcvd 10-4
Frames Txmtd 10-4
Port # 10-4
System Authentication Configuration screen 3-33
screen fields
Authentication Status 3-34
Authentication Type 3-34
Port # 3-34
System Authentication 3-34
System Resources Information screen 4-28
screen fields
CPU Type 4-29
Current Switch Utilization 4-29
DRAM Installed 4-29
FLASH Memory Installed 4-29
NVRAM Installed 4-29
Peak Switch Utilization 4-29
Reset Peak Switch Utilization 4-29

T

Tag 12-5
Tag Header 12-5
Tagged frame 12-5, 12-10
Telnet connections 2-4
TFTP Gateway IP Addr 4-5, 4-33
Traffic Class Configuration screen 8-10
screen fields
Priority 8-11
SAVE 8-11
SAVE TO ALL PORTS 8-11

Traffic Class 8-11
Traffic Class Information screen 8-7
screen fields
Port 8-9
Priority 8-9
Traffic Class to Port Priority
assignment of 8-11
Transmit Queues Configuration screen 8-12
screen fields
Current Queueing Mode 8-14
Number of Queues 8-14
Port 8-14
SET ALL PORTS 8-14
Weights Q0, Q1, Q2, Q3 8-14
Trap table configuration 4-22
Traps
enable 4-22

U

Uninterruptible Power Supply
COM configuration for 2-4
connection of 2-4
Untagged frame 12-5, 12-10

V

VLAN
assigning ports 12-8
components 12-7
configuration 12-7
default VLAN 12-5
defining 12-8
definition 12-2–12-4
Local Management for 6-3
operation 12-8
terms 12-4
types 12-3
VLAN Classification Configuration screen 7-21
screen fields
ADD 7-23
Classification 7-23
Classification (top of screen) 7-23
DEL ALL/DEL MARKED 7-23
Description (top of screen) 7-23
VID 7-23
VID (top of screen) 7-22
VLAN Configuration
deleting 7-10
VLAN ID 12-4
VLAN Local Management 7-2, 12-15
VLAN Port Configuration screen 7-17
screen fields
Acceptable Frame Type 7-19
Global GVRP State 7-19
GVRP Status 7-19
Ingress Filtering 7-19
Policy PVID Override 7-18
Port 7-19
Port Mode 7-19
PVID 7-19
VLAN Ports
configuration of 7-20
VLAN Redirect Configuration screen 5-19
screen fields
Destination Port 5-21
Destination Port [n] 5-21
Frame Format (Read-Only) 5-21
Frame Format (Selectable) 5-21
Redirect Errors 5-21
Source VLAN 5-21
Source VLAN [n] 5-21
Status 5-21
VLAN Spanning Tree
configuring a 6-8
VLAN Spanning Tree ports
configuration of 6-11

W

Weighted Queueing Mode
setting of 8-15